PATENT
0717-0518P

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant:	ZHANG, Xiaomang	Conf.:	
Appl. No.:	NEW	Group:	
Filed:	September 30, 2003	Examiner:	

For: ELECTRONIC SEAL, MEMORY MEDIUM, ADVANCED AUTHENTICATION SYSTEM, MOBILE DEVICE, AND VEHICLE START CONTROL APPARATUS

L E T T E R

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

September 30, 2003

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

Country	Application No.	Filed
JAPAN	2002-289228	October 1, 2002

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By _____
Terrell C. Birch, #19,382

P.O. Box 747
Falls Church, VA 22040-0747
(703) 205-8000

TCB/tmr
0717-0518P

Attachment(s)

ZHANG
BSKB LLP
703-205-8000
September 30, 200
0717-0518P
1 OF 1

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月　１日

出願番号
Application Number: 特願２００２－２８９２２８

[ST. 10/C]: [ＪＰ２００２－２８９２２８]

出願人
Applicant(s): シャープ株式会社

２００３年　９月　３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０７２００２

【書類名】　特許願
【整理番号】　02J02931
【提出日】　平成14年10月 1日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/00
G07D 7/00
【発明者】
【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内
【氏名】　張　小▲忙▼
【特許出願人】
【識別番号】　000005049
【氏名又は名称】　シャープ株式会社
【代理人】
【識別番号】　100078282
【弁理士】
【氏名又は名称】　山本　秀策
【選任した代理人】
【識別番号】　100062409
【弁理士】
【氏名又は名称】　安村　高明
【選任した代理人】
【識別番号】　100107489
【弁理士】
【氏名又は名称】　大塩　竹志
【手数料の表示】
【予納台帳番号】　001878
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0208587

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子印鑑、リムーバブルメモリ媒体、事前認証システム、携帯機器、携帯電話装置および車両始動制御装置

【特許請求の範囲】

【請求項１】　交信要求信号を生成する交信要求手段と、該交信要求信号を出力可能とすると共に、所定鍵に基づいて暗号化された乱数値を入力可能とする入出力手段と、該入出力手段で入力した乱数値を、所定鍵と関連した秘密鍵に基づいて復号した値を、該秘密鍵に基づいて暗号化する事前認証処理手段とを備え、該入出力手段は、事前認証処理手段で暗号化した乱数値を出力する電子印鑑。

【請求項２】　前記事前認証処理手段は、

前記秘密鍵を記憶する秘密鍵記憶手段と、

該秘密鍵記憶手段の秘密鍵に基づいて、前記入出力手段によって入力された乱数値を復号する復号手段と、

該秘密鍵記憶手段の秘密鍵に基づいて、該復号手段によって復号化された乱数値を暗号化する暗号化手段とを有する請求項１記載の電子印鑑。

【請求項３】　前記交信要求手段は、交信要求ＩＤ（Identification）を記憶する交信要求ＩＤ記憶手段と、操作指令に基づいて該交信要求ＩＤ記憶手段内の交信要求ＩＤを交信要求信号として読み出すデータ読出手段とを有する請求項１記載の電子印鑑。

【請求項４】　前記入出力手段は、相手側のリムーバブルメモリ媒体に対して電源供給可能とするリーダ／ライタ装置である請求項１記載の電子印鑑。

【請求項５】　前記所定鍵は公開鍵であり、前記秘密鍵は該公開鍵とＲＳＡ暗号化方式または楕円曲線暗号化方式を用いて鍵ペアを構成する請求項１記載の電子印鑑。

【請求項６】　交信要求信号を入力可能とする入出力手段と、該交信要求信号に基づいて起動信号を生成する起動信号生成手段と、該起動信号により所定鍵に基づいて乱数値を暗号化し、また、暗号化された乱数値を所定鍵に基づいて復号化して得られた値と該暗号化前の乱数値とが一致するかどうかを検出し、その検出結果を記憶する事前認証処理手段とを備え、該入出力手段は、該暗号化した

乱数値を出力可能とし、該暗号化された乱数値を入力可能とするリムーバブルメモリ媒体。

【請求項７】　前記事前認証処理手段は、

乱数値を発生する乱数値発生手段と、

所定鍵を記憶する所定鍵記憶手段と、

該乱数値発生手段によって発生させた乱数値を前記起動信号により暗号化を開始すると共に、該所定鍵に基づいて暗号化する暗号化手段と、

該所定鍵に基づいて、所定鍵と関連した秘密鍵に基づいて暗号化された乱数値を復号する復号手段と、

該乱数値発生手段によって発生させた乱数値と該復号手段よって復号化された乱数値とを比較して一致するかどうかを検出する第１比較手段と、

該第１比較手段による検出結果を記憶する検出結果記憶手段とを有する請求項６記載のリムーバブルメモリ媒体。

【請求項８】　前記起動信号生成手段は、交信要求ＩＤ（Identification）を記憶する交信要求ＩＤ記憶手段と、相手側からの交信要求ＩＤと交信要求ＩＤ記憶手段内の交信要求ＩＤを比較して一致した場合のみ起動信号を出力する第２比較手段とを備えた請求項６記載のリムーバブルメモリ媒体。

【請求項９】　前記入出力手段は、交信要求ＩＤを交信要求信号として受信可能とし、暗号化された乱数値を受信可能とする受信手段と、該暗号化した乱数値を相手側に送信可能とする送信手段とを有する請求項６記載のリムーバブルメモリ媒体。

【請求項１０】　前記所定鍵は公開鍵であり、前記秘密鍵は該公開鍵とＲＳＡ暗号化方式または楕円曲線暗号化方式を用いて鍵ペアを構成する請求項７記載のリムーバブルメモリ媒体。

【請求項１１】　アクセス要求に対して、前記検出結果が一致を示す所定値の場合にアクセス許可信号を出力し、該検出結果が該所定値以外の場合にアクセス禁止信号を出力するアクセス許可処理手段を更に備えた請求項７記載のリムーバブルメモリ媒体。

【請求項１２】　前記アクセス許可処理手段は、前記所定値の場合にアクセ

ス許可信号を出力すると共に、前記検出結果記憶手段に前記所定値以外の値を前記検出結果として記憶させる請求項１１記載のリムーバブルメモリ媒体。

【請求項１３】　請求項１記載の電子印鑑であって、少なくともメニュ画面および実行結果画面を表示可能とする表示部と、各種モードから所望のモードを選択可能とする選択・決定キーと、数字設定用キーと、選択モードを実行させるスタートキーとを有した電子印鑑。

【請求項１４】　外形形状がカード形状、円柱形状および角柱形状のいずれかである請求項１３記載の電子印鑑。

【請求項１５】　前記所定鍵および秘密鍵からなる鍵情報を外部から１回に限り入力して関連メモリに設定可能とする初期設定モード部と、該関連メモリに格納した所定鍵を出力して届印処理する届印モード部とを有した請求項１記載の電子印鑑。

【請求項１６】　前記事前認証処理手段による事前承認結果を取り消すために取消信号を出力する取り消しモード部を有する請求項１記載の電子印鑑。

【請求項１７】　使用有効期間を関連メモリに設定可能とし、設定された使用有効期間を外部に出力する期間設定モード部を有する請求項１記載の電子印鑑。

【請求項１８】　使用有効回数を関連メモリに設定可能とし、設定された使用有効回数を外部に出力する回数設定モード部を有する請求項１記載の電子印鑑。

【請求項１９】　１回に使うことができる金額の上限値を関連メモリに設定可能とし、設定された金額値を外部に出力する金額設定モード部を有した請求項１記載の電子印鑑。

【請求項２０】　前記表示部上に年月日時間を表示すると共に、前記数字設定用キーにより該年月日時間の時計表示の設定可能とする時計設定モード部を有した請求項１３記載の電子印鑑。

【請求項２１】　外部から入力された所定鍵情報を登録処理する初期設定モード部を有した請求項６記載のリムーバブルメモリ媒体。

【請求項２２】　前記初期設定モード部は、請求項１５記載の電子印鑑の届

印モード部による出力所定鍵情報を入力して関連メモリに設定する請求項２３記載のリムーバブルメモリ媒体。

【請求項２３】　外部からの取消信号によって前記事前認証処理手段による事前承認結果を取り消す取り消しモード部を有する請求項６記載のリムーバブルメモリ媒体。

【請求項２４】　外部から入力された使用有効期間を関連メモリに設定可能とし、使用有効期間を超えるとアクセス許可処理を禁止する期間設定モード部を有する請求項６記載のリムーバブルメモリ媒体。

【請求項２５】　外部から入力された使用有効回数を関連メモリに設定可能とし、該設定回数を超えるとアクセス許可処理を禁止する回数設定モード部を有する請求項６記載のリムーバブルメモリ媒体。

【請求項２６】　１回に使うことができる金額の上限値を外部から入力して関連メモリに設定可能とし、該設定金額を超えるとアクセス許可処理を禁止する金額設定モード部を有する請求項６記載のリムーバブルメモリ媒体。

【請求項２７】　請求項１～５、１３～２０の何れかに記載の電子印鑑と、請求項６～１２、２１～２６の何れかに記載のリムーバブルメモリ媒体とを備え、該リムーバブルメモリ媒体と電子印鑑とが互いにデータ交換することにより事前認証処理を行う事前認証システム。

【請求項２８】　前記リムーバブルメモリ媒体はＩＣカードまたはメモリカードである請求項２７記載の事前認証システム。

【請求項２９】　請求項１～５、１３～２０のいずれかに記載の電子印鑑が収納された携帯機器。

【請求項３０】　請求項１～５、１３～２０のいずれかに記載の電子印鑑が着脱自在に収納された携帯電話装置。

【請求項３１】　請求項２７または２８記載の事前認証システムにおいて、前記電子印鑑を収納した携帯機器と車体内の前記リムーバブルメモリ媒体との間で本人認証処理を前提として車の始動を可能とする車両始動制御装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、例えば市役所の窓口業務や電子商取引などで例えばＩＣカードやメモリカードなどに対して事前承認方式で本人認証を行う電子印鑑、これを使用可能とするＩＣカードおよびメモリカードなどのカード形式のリムーバブルメモリ媒体（着脱自在で携帯可能なメモリ媒体）、それらを用いた事前承認システム、この電子印鑑を収納した携帯機器、携帯電話装置および車両始動制御装置に関する。

【０００２】

【従来の技術】

従来、市役所の窓口、商取引などにおいて、本人認証は印鑑（伝統印鑑）の捺印によって行われている。印鑑は、盗難などに遭った場合に気づき易いため、早急に被害防止対策を講じることができる。

【０００３】

近年では、ＩＣカード、電子商取引、暗号化Ｅメールなどのように、情報が電子データ化（デジタルデータ化）されて流通されるようになってきており、それに伴って、本人認証の方法についても変化してきている。

【０００４】

ＩＣカード、ＩＤカード、電子商取引、暗号化Ｅメールなどにおいて、セキュリティ機能としては非常に強固なものが要求されるが、そのセキュリティ機能は、例えば４桁の暗証番号などのように、非常に脆弱な手段によって守られている。

【０００５】

例えば、電子財布として利用されるＩＣカード（Ｓｍａｒｔ　Ｃａｒｄとも称される）には、クレジットカードとキャッシュカードとがあり、クレジットカードの場合にはＩＣカードによるセキュリティチェックと筆記署名の目視確認という二つの要素で本人認証が行われ、キャッシュカードの場合にはＩＣカードによるセキュリティチェックと暗証番号の入力確認という二つの要素で本人認証が行われる。

【０００６】

しかしながら、模倣署名を目視判断で見破ることは容易ではなく、暗号番号は4桁の数字であるために安全性が低い。さらに安全性を高めるために、暗証データの桁数を増やすと、利用者の記憶に負担を強いることになる。

【０００７】

ＩＣカードの安全性を高めるためには、署名、指紋、声紋、網膜パターン、顔などといった利用者固有の情報に基づいて本人認証を行う方法が考えられるが、そのアルゴリズムなどのソフト面や装置などのハード面からユーザ操作手数などの運営面までを考えると、それをＩＣカードが利用される現場で応用することは容易ではない。

【０００８】

また、ＩＣカードは、主として欧米において、携帯電話器、ケーブルテレビジョン装置などの課金に対しても利用されており、そのセキュリティチェックは利用者に提供されるＰＩＮナンバーによって行われている。このため、上記暗証番号と同様に、安全性の面で問題がある。

【０００９】

また、入退室管理カードのようなＩＤカードは広く用いられているが、ＩＤカードによって確認するだけで本人と認められることが多い。しかしながら、このようなＩＤカードは、紛失・盗難などによって、簡単に悪用され得る。

【００１０】

また、電子商取引における安全性は、認証局によって証明書が発行された専用Ｗｅｂブラウザに依存している。その専用Ｗｅｂブラウザを利用するためには暗証番号が必要であるが、その暗証番号が漏れると、ブラウザ内部のセキュリティは強固であっても、誰でもアクセスすることができるようになる。

【００１１】

暗号化Ｅメールについては、暗号化関連の鍵などが計算機によって管理されているため、その計算機を利用する人であれば、自由に暗号化メールを読み書きすることができる。

【００１２】

図１３は、従来の本人認証システムの一例を示すブロック図である。

【００１３】

図１３において、この本人認証システム１１０は、カード関連内容のバックアップをしている遠隔サーバ１１１と、例えば相関情報、セキュリティ処理情報および暗証番号照合情報などが記憶されたＩＣカード１１２と、サービス内容表示処理、選択実行処理、セキュリティ処理および暗証番号入力処理などの各種処理を行うホストコンピュータ１１３と、ＩＣカード１１２とホストコンピュータ１１３の交信インターフェイスおよび、非接触カードへの電源供給を行うとカードリーダ／カードライタ１１４と、暗証番号などの入力装置１１５とを備え、ＩＣカードをキャッシュカードとして用いる場合などに本人認証を行う。

【００１４】

遠隔サーバ１１１には、ＩＣカード１１２に関する情報がバックアップ保存されているが、遠隔サーバ１１１にアクセスするためにはリアルタイム通信が必要であるため、本人認証は、ＩＣカード１１２とホストコンピュータ１１３の間および、ユーザとホストコンピュータ１１３の間で行われる。

【００１５】

ＩＣカード１１２およびホストコンピュータ１１３はセキュリティ機能を有しており、ＩＣカード１１２が接触型である場合には、インターフェイスとしてのカードリーダ／カードライタ１１４を介してＩＣカード１１２とホストコンピュータ１１３との間で互いにセキュリティチェックのためにデータ交信が行われる。

【００１６】

また、ＩＣカード１１２が非接触型である場合には、カードリーダ／カードライタ１１４からＩＣカード１１２に対して電源が供給され、ホストコンピュータ１１３とＩＣカード１１２との間で互いにセキュリティチェックのためにデータ交信が行われる。

【００１７】

そのセキュリティチェックにおいて、ホストコンピュータ１１３がそのＩＣカード１１２を真性であると確認すると、ホストコンピューター１１３のディスプレイに暗証番号入力画面が表示される。

【００１８】

次に、ユーザによって暗証番号が入力装置１１５から入力されると、入力された暗証番号がホストコンピューター１１３からカードリーダ／カードライタ１１４を介してＩＣカード１１２に供給され、ＩＣカード１１２の内部で暗証番号の照合が行われる。この暗証番号の照合結果によって本人と確認されると、ＩＣカード１１２の使用が認められる。ユーザによってサービス内容が選択されると、ホストコンピュータ１１３によってそのサービスが実行されて、ホストコンピュータ１１３のディスプレイにサービス内容が表示される。

【００１９】

【特許文献１】

特開平３－９２９６６号公報「電子財布システム」

【００２０】

【発明が解決しようとする課題】

本発明者らが関連特許出願（特願２００２－２２５５９０号）で提案した電子印鑑がＩＣカードの本人認証に使われる場合、その仕組みを図１３および図１４に示している。

【００２１】

図１４は、本発明者らが関連特許出願で提案した本人認証システムの一実施形態における要部構成を示すブロック図である。

【００２２】

図１４において、本人認証システム２００は、遠隔サーバ２１１と、ＩＣカードやメモリカードなどのカード２１２と、ホストコンピュータ２１３と、カードリーダー・ライター２１４と、　暗証番号などの入力装置２１５と、電子印鑑２１６とを有しており、カード２１２をキャッシュカードとして使う場合に電子印鑑２１６を用いて本人認証を行うようになっている。

【００２３】

遠隔サーバ２１１にはカード２１２の情報をバックアップして保存しているが、遠隔サーバ２１１のアクセスにリアルタイム通信が必要となる。このため、認証などのやり取りはホストコンピュータ２１３とカード２１２と電子印鑑２１６

との間で行われる。

【００２４】

まず、ＩＣカード２１２とホストコンピュータ２１３との間でセキュリティチェックを行う。お互いに認めてから、ホストコンピュータ２１３のディスプレイに対して暗証番号入力装置２１５から暗証番号を入力し、入力した暗証番号をカードリーダー・ライター２１４を経由してＩＣカード２１２に送られ、ＩＣカード２１２の内部で暗証番号の照合を行う。

【００２５】

次に、ホストコンピュータ２１３はカードリーダー・ライター２１４を経由し、ＩＣカード２１２に支払いための情報アクセス要求を出力する。ＩＣカード２１２はホストコンピュータ２１３の情報アクセス要求に応じる前に、カードリーダー・ライター２１４を通して、電子印鑑２１６により本人であるかどうかを認証する本人認証を行う。ＩＣカード２１２は電子印鑑２１６が本人の印鑑であると認めたら、ＩＣカード２１２がホストコンピュータ２１３からの情報アクセス要求を許可する。また、ＩＣカード２１２は電子印鑑２１６が本人の印鑑であると認めなかったら、ＩＣカード２１２がホストコンピューター２１３からの情報アクセス要求を拒否する。

【００２６】

図１５は、図１４の本人認証システム２００において電子印鑑により本人認証を行う際に、ＩＣカードと電子印鑑との間に発生する処理内容を示すフローチャートである。

【００２７】

図１５に示すように、まず、ＩＣカード２１２側からの乱数Ｄ１をランダムに生成する（ステップＳ３０１）。

【００２８】

次に、生成された乱数Ｄ１と返信要求ＩＤとを公開鍵Ｋｐで暗号化した信号を、カードリーダー・ライター２１４を経由して電子印鑑２１６側に、カード会社のＩＤ番号と共に、公開鍵Ｋｐで暗号化された乱数Ｄ１と公開鍵Ｋｐで暗号化された返信要求ＩＤとを送信する（ステップＳ３０２）。

【００２９】

さらに、電子印鑑２１６側では、受信したカード会社のＩＤ番号から秘密鍵Ｋｓを特定する（ステップＳ３０３）。

【００３０】

さらに、公開鍵Ｋｐで暗号化された乱数Ｄ１と公開鍵Ｋｐで暗号化された返信要求ＩＤとを、ステップＳ３０３で特定した秘密鍵Ｋｓで復号化する。これにより、複号化された送信要求ＩＤと複号化された乱数Ｄ２とが得られる（ステップＳ３０４）。

【００３１】

さらに、複号された送信要求ＩＤが含まれているか否かを判断する（ステップＳ３０５）。判断した結果、送信要求ＩＤが含まれていない場合は、その時点で、処理を終了する（ステップＳ３０６）。また、判断した結果、送信要求ＩＤが含まれている場合には、複合化された乱数Ｄ２をステップＳ３０３で特定した秘密鍵Ｋｓで暗号化して、暗号化された乱数Ｄ３をＩＣカード側に送り返す（ステップＳ３０７）。

【００３２】

ＩＣカード２１２側では、受信した暗号化された乱数Ｄ３を公開鍵Ｋｐで復号した乱数Ｄ３を得る（Ｓ３０８）。Ｓ３０１で生成した乱数Ｄ１とＳ３０８で得られた乱数Ｄ３との照合を行う（Ｓ３０９）。照合した結果、一致であれば本人と認める（Ｓ３１０）。照合した結果、不一致であれば、本人と認めない判断を下す（Ｓ３１１）。

【００３３】

この本人認証システム２００では、遠隔サーバー２１１に繋がるホストコンピュータ２１３と、ＩＣカード２１２と、電子印鑑２１６との３者が揃うことが、本人認証を行う必要条件である。

【００３４】

即ち、ＩＣカード２１２を使う度に電子印鑑２１６が使われるが、この場合の電子印鑑２１６とカードリーダー・ライター２１４との交信距離が遠距離（例えば１メートル以上）の場合には、電子印鑑２１６をＩＣカード２１２と一緒に提

出しなくても本人認証に支障を与えない。ところが、電波法の規制や省エネルギーにより非接触交信方式であっても交信距離は７０ｃｍ以内である。このとき、交信を確実に行うために、ＩＣカード２１２をクレジットカードとして使う場合に、電子印鑑２１６をＩＣカード２１２と一緒に操作店員さんに渡す必要が生じ、ＩＣカード２１２の１枚だけ操作店員さんに渡す伝統的な従来の使い方に比べて操作手数が増える。

【００３５】

また、電子印鑑２１６にカード会社のＩＤ番号を登録する必要がある。ＩＣカード２１２を発行して貰うために、カード会社が電子印鑑２１６にその会社を識別するＩＤ番号を入力する。これにより、運営管理およびセキュリティの面で、色々な問題を生じる。運営管理の面においては、関連機関がカード会社や銀行を識別できるＩＤ番号の決定・公表・管理を実施することになり、これは莫大な作業である。カードを発行するとき、電子印鑑２１６にカード会社のＩＤ番号を組みこむことになり、本人認証の代わりに使う電子印鑑２１６へのデータの書き込みはセキュリティの観点から望ましくない。

【００３６】

さらに、前述したように、遠隔サーバ２１１に繋がるホストコンピュータ２１３と、ＩＣカード２１２と、電子印鑑２１６との３者が揃うことが、本人認証を行う上で必要条件であるため、認証フローが伝統的な電子印鑑を用いない場合に対してかなり変更を余儀なくされる部分がある。認証システムの変更により莫大な資金が必要となってしまう。

【００３７】

さらに、電子印鑑２１６をメモリカードに保存したデータのアクセス保護に使用するときには、本人認証にはパーソナルコンピュータと、メモリカードと、電子印鑑２１６との３者が揃う必要がある。電子印鑑を用いない伝統的なシステムに、電子印鑑２１６と交信するためのカードリーダー・ライター２１４の増設、認証処理部分の追加などを行う必要が生じる。

【００３８】

本発明は、上記従来の問題を解決するもので、電子印鑑にカード会社のＩＤ番

号を組み込むことなく、電子印鑑を届印としてカードに登録することにより、ＩＣカードを容易に発行でき、かつ、従来の電子印鑑を用いないシステムに対して新たなる改造や増設をすることなく、電子印鑑とカードによる事前の本人認証により処理相手に電子印鑑を渡さずに電子印鑑を高セキュリティでカードのアクセス保護に使用することができる電子印鑑、これを使用可能とするＩＣカードおよびメモリカードなどのリムーバブルメモリ媒体、それらを用いた事前認証システム、この電子印鑑を収納した携帯機器、携帯電話装置および車両始動制御装置を提供することを目的とする。

【００３９】

【課題を解決するための手段】

本発明の電子印鑑は、交信要求信号を生成する交信要求手段と、交信要求信号を出力可能とすると共に、所定鍵に基づいて暗号化された乱数値を入力可能とする入出力手段と、入出力手段で入力した乱数値を、所定鍵と関連した秘密鍵に基づいて復号した値を、秘密鍵に基づいて暗号化する事前認証処理手段とを備え、入出力手段は、事前認証処理手段で暗号化した乱数値を出力するものであり、そのことにより上記目的が達成される。

【００４０】

また、好ましくは、本発明の電子印鑑における事前認証処理手段は、秘密鍵を記憶する秘密鍵記憶手段と、秘密鍵記憶手段の秘密鍵に基づいて、入出力手段によって入力された乱数値を復号する復号手段と、秘密鍵記憶手段の秘密鍵に基づいて、復号手段によって復号化された乱数値を暗号化する暗号化手段とを有する。

【００４１】

さらに、好ましくは、本発明の電子印鑑における交信要求手段は、交信要求ＩＤ（Identification）を記憶する交信要求ＩＤ記憶手段と、操作指令に基づいて該交信要求ＩＤ記憶手段内の交信要求ＩＤを交信要求信号として読み出すデータ読出手段とを有する。

【００４２】

さらに、好ましくは、本発明の電子印鑑における入出力手段は、相手側のリム

ーバブルメモリ媒体に対して電源供給可能とするリーダ／ライタ装置である。

【００４３】

さらに、好ましくは、本発明の電子印鑑における所定鍵は公開鍵であり、秘密鍵は公開鍵とＲＳＡ暗号化方式または楕円曲線暗号化方式を用いて鍵ペアを構成する。

【００４４】

本発明のリムーバブルメモリ媒体は、交信要求信号を入力可能とする入出力手段と、交信要求信号に基づいて起動信号を生成する起動信号生成手段と、起動信号により所定鍵に基づいて乱数値を暗号化し、また、暗号化された乱数値を所定鍵に基づいて復号化して得られた値と暗号化前の乱数値とが一致するかどうかを検出し、その検出結果を記憶する事前認証処理手段とを備え、入出力手段は、暗号化した乱数値を出力可能とし、暗号化された乱数値を入力可能とするものであり、そのことにより上記目的が達成される。

【００４５】

また、好ましくは、本発明のリムーバブルメモリ媒体における事前認証処理手段は、乱数値を発生する乱数値発生手段と、所定鍵を記憶する所定鍵記憶手段と、乱数値発生手段によって発生させた乱数値を起動信号により暗号化を開始すると共に、所定鍵に基づいて暗号化する暗号化手段と、所定鍵に基づいて、所定鍵と関連した秘密鍵に基づいて暗号化された乱数値を復号する復号手段と、乱数値発生手段によって発生させた乱数値と復号手段よって復号化された乱数値とを比較して一致するかどうかを検出する第１比較手段と、第１比較手段による検出結果を記憶する検出結果記憶手段とを有する。

【００４６】

さらに、好ましくは、本発明のリムーバブルメモリ媒体における起動信号生成手段は、交信要求ＩＤ（Identification）を記憶する交信要求ＩＤ記憶手段と、相手側からの交信要求ＩＤと交信要求ＩＤ記憶手段内の交信要求ＩＤを比較して一致した場合のみ起動信号を出力する第２比較手段とを有する。

【００４７】

さらに、好ましくは、本発明のリムーバブルメモリ媒体における入出力手段は

、交信要求ＩＤを交信要求信号として受信可能とし、暗号化された乱数値を受信可能とする受信手段と、暗号化した乱数値を相手側に送信可能とする送信手段とを有する。

【００４８】

さらに、好ましくは、本発明のリムーバブルメモリ媒体における所定鍵は公開鍵であり、秘密鍵は公開鍵とＲＳＡ暗号化方式または楕円曲線暗号化方式を用いて鍵ペアを構成する。

【００４９】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、アクセス要求に対して、検出結果が一致を示す所定値の場合にアクセス許可信号を出力し、検出結果が所定値以外の場合にアクセス禁止信号を出力するアクセス許可処理手段を更に備える。

【００５０】

さらに、好ましくは、本発明のリムーバブルメモリ媒体におけるアクセス許可処理手段は、所定値の場合にアクセス許可信号を出力すると共に、検出結果記憶手段に所定値以外の値を検出結果として記憶させる。

【００５１】

また、好ましくは、本発明の電子印鑑において、請求項１記載の電子印鑑であって、少なくともメニュ画面および実行結果画面を表示可能とする表示部と、各種モードから所望のモードを選択可能とする選択・決定キーと、数字設定用キーと、選択モードを実行させるスタートキーとを有する。

【００５２】

さらに、好ましくは、本発明の電子印鑑の外形形状がカード形状、円柱形状および角柱形状のいずれかである。

【００５３】

さらに、好ましくは、本発明の電子印鑑において、所定鍵および秘密鍵からなる鍵情報を外部から１回に限り入力して関連メモリに設定可能とする初期設定モード部と、この関連メモリに格納した所定鍵を出力して届印処理する届印モード部とを有する。

【００５４】

さらに、好ましくは、本発明の電子印鑑における事前認証処理手段による事前承認結果を取り消すために取消信号を出力する取り消しモード部を有する。

【００５５】

さらに、好ましくは、本発明の電子印鑑において、使用有効期間を関連メモリに設定可能とし、設定された使用有効期間を外部に出力させる期間設定モード部を有する。

【００５６】

さらに、好ましくは、本発明の電子印鑑において、使用有効回数を関連メモリに設定可能とし、設定された使用有効回数を外部に出力させる回数設定モード部を有する。

【００５７】

さらに、好ましくは、本発明の電子印鑑において、１回に使うことができる金額の上限値を関連メモリに設定可能とし、設定された金額値を外部に出力する金額設定モード部を有する。

【００５８】

さらに、好ましくは、本発明の電子印鑑において、表示部上に年月日時間を表示すると共に、数字設定用キーにより年月日時間の時計表示の設定可能とする時計設定モード部を有する。

【００５９】

また、好ましくは、本発明のリムーバブルメモリ媒体において、外部から入力された所定鍵情報を登録処理する初期設定モード部を有する。

【００６０】

さらに、好ましくは、本発明のリムーバブルメモリ媒体における初期設定モード部は、請求項１５記載の電子印鑑の届印モード部による出力所定鍵情報を入力して関連メモリに設定する。

【００６１】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、外部からの取消信号によって事前認証処理手段による事前承認結果を取り消す取り消しモー

ド部を有する。

【００６２】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、外部から入力された使用有効期間を関連メモリに設定可能とし、この使用有効期間を超えるとアクセス許可処理を禁止する期間設定モード部を有する。

【００６３】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、外部から入力された使用有効回数を関連メモリに設定可能とし、この設定回数を超えるとアクセス許可処理を禁止する回数設定モード部を有する。

【００６４】

さらに、好ましくは、本発明のリムーバブルメモリ媒体において、１回に使うことができる金額の上限値を外部から入力して関連メモリに設定可能とし、この設定金額を超えるとアクセス許可処理を禁止する金額設定モード部を有する。

【００６５】

本発明の事前認証システムは、請求項１～５、１３～２０の何れかに記載の電子印鑑と、請求項６～１２、２１～２６の何れかに記載のリムーバブルメモリ媒体とを備え、このリムーバブルメモリ媒体と電子印鑑とが互いにデータ交換することにより事前認証処理を行うものであり、そのことにより上記目的が達成される。

【００６６】

また、好ましくは、本発明の事前認証システムにおけるリムーバブルメモリ媒体はＩＣカードまたはメモリカードである。

【００６７】

本発明の携帯機器は、請求項１～５、１３～２０のいずれかに記載の電子印鑑が収納されたものであり、そのことにより上記目的が達成される。

【００６８】

本発明の携帯電話装置は、請求項１～５、１３～２０のいずれかに記載の電子印鑑が着脱自在に収納されたものであり、そのことにより上記目的が達成される。

【００６９】

本発明の車両始動制御装置は、請求項２７または２８記載の事前認証システムにおいて、電子印鑑を収納した携帯機器と車体内のリムーバブルメモリ媒体との間で本人認証処理を前提として車の始動を可能とするものであり、そのことにより上記目的が達成される。

【００７０】

上記構成により、以下、本発明の作用について説明する。

【００７１】

まず、現状から順をおって説明する。例えば旧来の銀行のキャッシュカードや、ＩＣカード、メモリカードなどのリムーバブルメモリ媒体としてのカード類を使う場合には、例えば４桁の暗証番号のみを予め決めておいて、ユーザがカードを使用するときに、そのカードを装置に挿入してから、この暗証番号を入力することで、本人認証を行っている。

【００７２】

しかしながらこのような４桁の暗証番号では、コンピュータを用いて解析すれば、簡単にセキュリティを破られてしまう。つまり、現状の暗証番号による本人認証システムは、既に問題を抱えており、何らかの対策が必要な状況となっている。

【００７３】

例えばＩＣカードをクレジットカードとして使う場合には、通常は暗証番号さえ使わずに支払う様になっている。この時に、使用者に署名をさせることで、本人認証を行うことはできる。しかし、人が目視で署名の真偽を鑑別することは非常に困難である。即ち、現状ではＩＣカードは本人でなくとも、これを取得した人は誰でも、何の不自由なく使用することが可能である。

【００７４】

例えばメモリカード（例えばCF, Smart Media（登録商標）, SD, MemoryStick（登録商標）などと呼ばれているものなど）は近年、大容量かつ小型化になりつつあり、しかもその記憶内容は個人のプライバシー情報（顔写真、金融、証券、健康データ等）に深く関わっている。しかも、これら小型化のメモリカードは紛

失しやすく、容量が大きいので被害リスクが高くなる。現状においては、このようなメモリカードは、誰でもその内容を読み出すことが可能である。即ち、現状ではメモリカードのセキュリティ対策は充分に考慮されていない。

【００７５】

例えばキャッシュカードに関して、これらの問題に対する一つの解決策としては、暗証番号の桁数を大きくすることで、取り敢えずのセキュリティは確保できる。しかし、暗証番号の桁数は増やせば増やすほどセキュリティを破るのは難しくなり、その意味では望ましい方向であるが、桁数の多い暗証番号をユーザが覚えておくことは煩雑でもあり、更に暗証番号は度々変更しておかなければならないという事情があり、ユーザの使い勝手は悪くなると言う問題点を持っている。同様に、クレジットカードやメモリカードに対しても、それなりのセキュリティ対策を講じる必要がある。

【００７６】

このようなカード類（ここでは単にカードと総称している）を使う上での事情を考慮して、一つのセキュリティを確保できるシステムとして、次に述べるようなものが提案された。それは基本的に述べると、本人認証のために、電子印鑑とカード（例えばＩＣカードまたはメモリカード、キャッシュカードなど）とホストコンピュータの、大きく分けて三つが揃って初めて、本人の認証が出来る前述した本人認証システム（特願２００２－２２５５９０号）である。

【００７７】

ここで、電子印鑑は本人認証の為に使われるもので、イメージ的にはＩＣカードに対する第２カードのようなものである。ＩＣカードも電子印鑑も、暗号化された鍵情報を使って、本人認証を行う。従って、このように三つが揃って初めて、ユーザ本人がカードを使うことができるので、セキュリティ面では極めて安全と言うことができる。

【００７８】

しかしながら、この本人認証システム（特願２００２－２２５５９０号）には、次のような課題がある。つまり、この本人認証システムでは従来のカード使用のシステム構成を大幅に変更することになり、そのための設備投資が大掛かりに

なることと、ユーザにとっては一々カードと電子印鑑とを持ち歩かなくてはならないという使い勝手の悪さとが課題としてある。

【００７９】

そこで、本発明においては、このような従来のシステム自体を変更せずに、従来のカードシステムと共存できて、なおかつ高度なセキュリティを確保できる方式として、公開鍵と秘密鍵による鍵ペアを用いてカード（例えばＩＣカードまたはメモリカード、キャッシュカードなど）と電子印鑑とを直に交信可能とすることによりカード（例えばＩＣカードまたはメモリカード、キャッシュカードなど）を事前に電子印鑑で本人認証を行った上で、１回に限り使用できるようにしたものである。

【００８０】

事前認証を行うための具体的構成について説明すると、電子印鑑およびカードは次のように構成されている。即ち、電子印鑑側からカードに対して交信要求（ＩＤ）を送信し、カードはこれをチェックする。チェックがＯＫであれば、カードの事前認証部分では、ランダム乱数を発生させ、これを公開鍵で暗号化して、電子印鑑側に送り、電子印鑑はこの受け取りデータを秘密鍵で復号化し、さらに秘密鍵で暗号化してＩＣカードに送る。このデータを受け取ったＩＣカードは、又公開鍵で復号化する。このときに、公開鍵データ（ＩＣカード側）と、秘密鍵データ（電子印鑑側）とは理論的に常に鍵ペアを構成している。乱数を暗号化して交信することも本発明の特長の一つである。

【００８１】

例えばＩＣカードの場合、電子印鑑にその人しか持てない鍵情報を登録し、電子印鑑をカスタマイズする。登録は１回しか行なえない。未登録電子印鑑は鍵情報がオール１である。オール１であるときにのみ、登録が可能である。カスタマイズ済みの電子印鑑を届印として、金融機関に提出し、金融機関が電子印鑑に格納してある公開鍵情報を、ＩＣカードに登録してＩＣカードを発行して貰う。この登録も１回しか実施できない。また、電子印鑑側にカードリーダ・ライタと電池を内蔵すれば、電子印鑑とＩＣカードとの間で直に交信が可能となる。ユーザ本人だけでも、電子印鑑を使ってＩＣカードに事前の本人認証を行うことが可能

となる。このようにすれば、事前承認済みのＩＣカードが伝統的なＩＣカード金融システムでも使うことができる。もちろん、事前承認の無いＩＣカードは使えない。

【００８２】

例えばメモリカードの場合、カスタマイズ済みの電子印鑑を使って、ユーザ本人がメモリカードに電子印鑑の公開鍵を登録する。この登録も１回しか実施できないようにする。ユーザ本人が電子印鑑を使ってメモリカードに事前承認を行う。事前承認済みのメモリカードには汎用のパソコンなどでアクセスできる。もちろん、事前承認の無いメモリカードにはアクセスができない。メモリカードは従来のシステムで従来の通りに使用可能である。

【００８３】

このように、事前に本人認証を終えたカードは、一度だけホストコンピュータと交信できる。即ち一度だけなら、カード使用時点で事前の本人認証をせずにカードを使用できる。以後このカードは、使用の度に事前承認手続き（即ち、電子印鑑での承認）をしておけばよく、電子印鑑を持ち運ぶ必要がなくなる。

【００８４】

したがって、電子印鑑にカード会社のＩＤ番号を組み込むことなく、電子印鑑を届印としてカードに登録してＩＣカードを容易に発行でき、かつ、従来の電子印鑑を用いないシステムに対して新たなる改造や増設をすることなく、相手に電子印鑑を渡さずに電子印鑑とカードによる事前の本人認証を行って、電子印鑑を高セキュリティでカードのアクセス保護に使用することが可能となる。

【００８５】

次に、この電子印鑑とは、「印鑑」と言う言葉があるので表現として誤解を与える可能性もあるが、要するに「個人認証のために、相手（ここではカード類）と鍵情報を用いて、データを乱数によって暗号化及び復号化処理することで交信して、個人認証を行う装置」である。この場合、装置がハンディ型で、簡単に持ち運びできることが重要で、第２のカードのようなものである。その意味では、電子印鑑の適用相手として、何もカード類に限る必要はなく、例えば販売機に対して直接電子印鑑で本人認証を行って、その場で物を購入できるようにしてもよ

いし（電子マネー）、有料テレビ、ゲーム機、電話装置などで使えるようにすることもできる。さらには、今回の電子印鑑機能を、常日頃使用者が持ち歩いているような道具類、例えば携帯電話機（電子印鑑の普及を目的として携帯電話機に外部から組み込む場合など）、車のキー（車の盗難防止対策として用いる場合など）、腕時計、ＰＤＡなどに搭載しておけば、これらの道具に搭載された電子印鑑機能を使って個人認証を行うことができるので、使い勝手は格段に向上する。即ち、市場規模として非常に大規模になると考えられる。

【００８６】

【発明の実施の形態】

以下に、本発明の事前認証システムの実施形態１，２について図面を参照しながら説明する。

（実施形態１）

図１は、本発明の事前認証システムの実施形態１における要部構成を示すブロック図である。なお、ここでは、各要部毎の動作を示すフローチャートをも示している。

【００８７】

図１において、この事前認証システム１は、遠隔サーバ２と、ホストコンピュータ３（またはパーソナルコンピュータ；以下パソコンという）と、カードとの交信インターフェースである入出力手段としてのリーダー・ライター装置としてのカードリーダ／カードライタ４と、秘密鍵による本人認証機能を持つ電子印鑑５と、秘密鍵と鍵ペアの公開鍵による本人認証機能を持つリムーバブルメモリ媒体としてのＩＣカードやメモリカードなどのカード６とを備えている。

【００８８】

遠隔サーバ２には、各種カード関連情報がバックアップ保存されている。

【００８９】

ホストコンピュータ３は、入力装置３１による入力指示によりカード６に対してカードアクセス要求処理が為され、セキュリティ処理として本人であることが認められた場合のみ遠隔サーバ２やカード６内の個人情報などと交信可能となり、ユーザ選択実行処理後に所望のカード関連情報を、サービス内容出力処理とし

て画面表示させたりプリントアウトさせたりできるようになっている。この本人認証は、遠隔サーバ２にアクセスするためにはリアルタイム通信が必要であるため、ホストコンピュータ３、電子印鑑５およびカード６の３者間で行われる。即ち、詳細には後述するが、電子印鑑５とカード６間の公開鍵方式暗号技術によって本人認証が行われ、ホストコンピュータ３とカード６との間で本人であることが確認されると、カード６の使用が認められ、ホストコンピュータ３のディスプレイ上にサービス内容が表示可能とされる。ユーザによって入力装置３１からサービス内容が選択されると、ホストコンピュータ３によってそのサービスが実行されるようになっている。

【００９０】

カードリーダ／カードライタ４は、非接触／接触用のカード６への電源供給を行うと共に、例えばホストコンピュータ３とカード６との間で互いにセキュリティ処理のためにデータ交信が行われる。このカードリーダ／カードライタ４の一例について図２にその詳細構成を示している。

【００９１】

図２は、図１のカードリーダ／カードライタ４の要部構成例を示すブロック図である。なお、このカードリーダ／カードライタ４はホストコンピュータ３とカード６間の交信インターフェースの他に、後述するが、別途、電子印鑑５に内蔵されて設けられており、電子印鑑５とカード６との間での交信インターフェースとしても働く。

【００９２】

図２において、カードリーダ／カードライタ４は、変調回路４１と、復調回路４２と、アンテナ４３と、不揮発性メモリ４４と、信号処理装置４５と、制御回路４６と、入出力Ｉ／Ｆ回路４７とを有しており、ホストコンピュータ３とカード６との間で非接触交信（無線による送受信）を担う。

【００９３】

変調回路４１は、信号処理回路４５からの信号が所定のキャリア波に変調されてアンテナ４３に供給される。例えば１３．５６ＭＨＺのキャリア波がＡＳＫ（Amplitude Shift Keying）方式でアンテナ４３から送信される。

【００９４】

復調回路４２は、アンテナ４３からの所定のキャリア波を復調して信号処理回路４５に供給する。

【００９５】

信号処理装置４５は、制御回路４６からの制御に基づいて、カード１２とホストコンピュータ３（または電子印鑑５）のデータ入出力が検出され、データ通信の際に送受信される信号が処理される。

【００９６】

制御回路４６は、内部にＣＰＵ（中央演算処理装置）およびメモリなどを有しており、不揮発性メモリ４４に予め記録されている制御プログラムを読み込んでそれを起動させることにより、カードリーダ／カードライタ４を構成する各回路部を制御する。また、制御回路４６は、入出力Ｉ／Ｆ回路４７を介して、ホストコンピュータ３などの上位装置とのデータ通信が行われ、また、電子印鑑５に内蔵されているカードリーダ／カードライタ４の場合には、電子印鑑５のセキュリティ処理部とのデータ通信が行われる。

【００９７】

次に、電子印鑑５は、内蔵されたカードリーダ／カードライタ５Ａと、カードリーダ／カードライタ５Ａとデータ交信して事前認証処理を担う本発明の事前認証処理手段を構成するセキュリティ処理部５Ｂとを有している。なお、このカードリーダ／カードライタ５Ａは、前述したカードリーダ／カードライタ４とその構成が同一であるため、ここではその説明を省略する。

【００９８】

セキュリティ処理部５Ｂの一例について図３に詳細に示している。

【００９９】

図３は、図１の電子印鑑５におけるセキュリティ処理部５Ｂの要部構成例を示すブロック図である。

【０１００】

図３において、電子印鑑５のセキュリティ処理部５Ｂは、電源電圧を発生する電源部としての電池５１と、交信要求ＩＤ記憶部５２と、秘密鍵記憶部５３と、

復号手段５４と、暗号化手段５５とを有している。

【０１０１】

電池５１は、電子印鑑５の電源として用いると同時に、カードリーダ／カードライタ５Ａを通してワイヤレスでカード６に対して電源を提供する。

【０１０２】

交信要求ＩＤ記憶部５２は交信要求手段を構成している。この交信要求手段は、交信要求ＩＤ（Identification）を記憶する交信要求ＩＤ記憶手段と、操作指令に基づいて交信要求ＩＤ記憶手段内の交信要求ＩＤを交信要求信号として読み出すデータ読出手段とから構成されており、記憶した交信要求ＩＤを読み出して電子印鑑５側からカード６側に送り、カード６に対して電子印鑑５との交信を要求する。

【０１０３】

秘密鍵記憶部５３は、後述する公開鍵と所定の鍵ペアを構成する秘密鍵情報を記憶しており、秘密鍵情報を各所定のタイミングで復号手段６４および暗号化手段６５に出力する。

【０１０４】

復号手段５４は、カード６側が交信要求ＩＤによる交信要求に応じて、詳細に後述するが公開鍵で暗号化し、送信してきた受信暗号化乱数の値を、秘密鍵鍵記憶部６３の秘密鍵を用いて復号する。

【０１０５】

暗号化手段５５は、復号した乱数の値を再び暗号化する。復号した乱数の値を秘密鍵記憶部６４の秘密鍵を使って再び暗号化して、カードリーダ／カードライタ５Ａを通してカード６側に送信する。

【０１０６】

次に、カード６の内部構成の一例について説明する。

【０１０７】

カード６は、カードリーダ／カードライタ４（または５Ａ）と交信可能な入出力手段としての図４の送受信・整流・ロジック回路６Ａと、本発明の事前認証処理手段としての図５のセキュリティ処理部６Ｂと、本発明のアクセス許可処理手

段としての図６のアクセス許可処理部６Ｃとを有している。この場合、カード６は、ＩＣカードやメモリカードなど各種カード類が考えられる。電子印鑑５に従来のようにカード会社のＩＤ番号を組み込むことなく、電子印鑑５を届印としてカード６側に登録（鍵ペア）することにより、カード６を発行することができる。また、ＩＣカードについては、事前承認処理が済んであれば、カード６内部のアクセス許可処理を意識しなくても従来通りに使える。そうでなければ、ホストコンピュータ３によってＩＣカードの使用は拒否される。また、メモリカードについては、事前承認処理が済んであれば、従来通りにメモリへのアクセスができる。そうでなければ、ホストコンピュータ３によってメモリカードへのアクセスは拒否される。

【０１０８】

図４は、図１のカード６に内蔵する送受信・整流・ロジック回路６Ａの要部構成例を示すブロック図である。

【０１０９】

図４において、カード６の送受信・整流・ロジック回路６Ａは、アンテナ６１と、整流回路６２と、クロック抽出回路６３と、復調回路６４と、定電圧発生回路６５と、パワーオンリセット回路５６と、変調回路６７と、内部ロジック６８とを有し、カード６と電子印鑑５またはホストコンピュータ３との非接触交信を担っている。なお、これらのアンテナ６１、整流回路５２、クロック抽出回路６３および復調回路６４により入力手段（ここでは受信手段であるが、接触型の場合を含んでいる）が構成され、また、アンテナ６１、整流回路６２、変調回路６７および内部ロジック回路６８により出力手段（ここでは送信手段であるが、接触型の場合を含んでいる）が構成されている。これらの入力手段および出力手段（受信手段および送信手段）により入出力手段（送受信手段）を構成している。

【０１１０】

アンテナ６１は送受信手段であり、カードリーダ／カードライタ４または５Ａからの信号が受信され得ると共に、カード６からの出力信号がカードリーダ／カードライタ４または５Ａ側に送信され得る。

【０１１１】

整流回路６２では、アンテナ６１を介して受信された信号を整流してクロック抽出回路６３および復調回路６４に出力し、また、変調回路６７からの信号を整流してアンテナ６１に出力する。

【０１１２】

クロック抽出回路６３は、アンテナ６１を介して受信されたカードリーダ／カードライタ４からのキャリア波から動作に必要なクロック信号が抽出され、内部ロジック回路６８に出力する。

【０１１３】

復調回路６４では、送受信手段であるアンテナ６１を介して受信されたカードリーダ／カードライタ４からの信号が復調されて内部ロジック回路６８に出力する。

【０１１４】

定電圧発生回路６５では、定電圧を発生してパワーオンリセット回路６６および内部ロジック回路６８に出力する。

【０１１５】

パワーオンリセット回路６６は、カード６の電源遮断／リセットを制御する回路であり、内部ロジック回路６８に電源遮断／リセットのための制御信号を出力する。

【０１１６】

変調回路６７では、内部ロジック回路６８による制御に基づいて、所定のキャリア波が任意の波長に変調され、アンテナ６１を介してカードリーダ／カードライタ４に送信される。

【０１１７】

内部ロジック回路６８は、ＣＰＵ（中央演算処理装置）および、ＲＯＭおよびＲＡＭからなるメモリなどを有しており、カード６を構成する各回路を制御する。　なお、以上のアンテナ６１～変調回路６７の構成は、カードリーダ／カードライタ４または５Ａとカード６とが非接触型で交信する場合の一例を示したが、この構成に限定されるものではなく、カードリーダ／カードライタ４または５Ａとカード６とが接触型で交信する場合として、図４の以外の構成を用いることも

可能である。

【０１１８】

図５は、図１のカード６におけるセキュリティ処理部６Ｂの要部構成例を示すブロック図である。

【０１１９】

図５において、カード６側の事前承認処理部であるセキュリティ処理部６Ｂは、交信要求ＩＤ記憶部７１と、比較手段７２（第２比較手段）と、乱数発生手段７３と、乱数記憶部７４と、公開鍵記憶部７５と、暗号化手段７６と、復号手段７７と、比較手段７８（第１比較手段）と、比較結果記憶手段としてのＦＬＡＧ記憶部７９とを有している。

【０１２０】

交信要求ＩＤ記憶部７１は、交信要求ＩＤ（Identification）を記憶する交信要求ＩＤ記憶手段と、交信要求ＩＤ記憶手段内の交信要求ＩＤを読み出すデータ読出手段とから構成されている。なお、この交信要求ＩＤは電子印鑑５側の交信要求ＩＤ記憶部５２にも記憶させているが、交信要求ＩＤの設計については暗号化した交信要求ＩＤ番号を使うことで、電子印鑑５の特定や実行の高速化に効果が得られる。例えば、全ての電子印鑑５の交信要求ＩＤを例えば「Ｌｅｔ’ｓＳｔａｒｔ」とすると、秘密鍵により暗号化した「Ｌｅｔ’ｓＳｔａｒｔ」を交信要求ＩＤとして電子印鑑５に登録する。暗号化した交信要求ＩＤの内容は電子印鑑５毎に異なるので、電子印鑑５の特定を容易にでき、電子印鑑５とカード６との交信スタートが簡単に制御できる。また、暗号化した交信要求ＩＤをそのまま使うことにより、復号の時間は不要となり、演算の高速化や省エネにも効果がある。

【０１２１】

比較手段７２は、電子印鑑５から受信したデータ（交信要求ＩＤ）と交信要求ＩＤ記憶部７１の交信要求ＩＤとを比較し、その比較結果が一致すれば、暗号化手段７５による暗号化処理を実行し、また、その比較結果が一致しなければ、セキュリティ処理を終了する。即ち、比較手段７２は、電子印鑑５側からの交信要求ＩＤと交信要求ＩＤ記憶手段７１内の交信要求ＩＤを比較して一致した場合の

み暗号化手段７６に起動信号を出力する。これらの交信要求ＩＤ記憶部７１および比較手段７２により起動信号生成手段が構成されている。

【０１２２】

乱数発生手段７３は乱数を発生する。この乱数発生は公知の擬似乱数発生方法（例えばＦＩＰＳ　ＰＵＢ　１８６－２に提案されているハッシュ関数ＳＨＡ－１を用いた乱数発生方法）が使える。

【０１２３】

乱数記憶部７４は乱数発生手段７３で発生した乱数を格納する。

【０１２４】

公開鍵記憶部７５は公開鍵情報を記憶する。

【０１２５】

暗号化手段７６は、乱数記憶部７４からの記憶乱数の値を、公開鍵記憶部７５からの公開鍵で暗号化し、送受信・整流・ロジック回路６Ａを経て電子印鑑５側に送信する。ここで用いる暗号化方式としては例えば後述のＲＳＡが使える。

【０１２６】

復号手段７７は、電子印鑑５側から受信したデータを復号する。この復号の際に公開鍵記憶部７５の公開鍵情報を使う。

【０１２７】

比較手段７８は、復号手段７７で復号したデータを乱数記憶部７４に記憶している乱数の値と比較し、その比較結果が一致すれば、事前承認が有効であると判断してＦＬＡＧ記憶部７９に「１」を設定し、また、その比較結果が一致しなければ、事前承認は無効であると判断してＦＬＡＧ記憶部７９に「０」を設定する。

【０１２８】

ＦＬＡＧ記憶部７９は事前承認の比較結果状態を、事前承認有効を示す「１」または事前承認無効を示す「０」で記憶する。

【０１２９】

図６は、図１のカード６におけるアクセス許可処理部６Ｃの要部構成例を示すブロック図である。

【０１３０】

図６において、カード６のアクセス許可処理部６Ｃは、外部バスロック手段８１と、比較手段８２と、外部バスロック解除手段８３と、不揮発性メモリ８４と、外部バス制御部８５とを有している。

【０１３１】

外部バスロック手段８１は外部バスをアクセス（内部からのデータ書き込み、データ読み出し）不能にする。即ち、外部バスロック手段８１は、ホストコンピュータ３（または汎用パーソナルコンピュータ）から、内蔵する送受信・整流・ロジック回路６Ａを経由して、不揮発性メモリ８５に対してアクセスしようとするときに、内蔵する送受信・整流・ロジック回路６Ａのパワーオンリセット回路６６の信号をトリガーとして外部バス制御手段８５を介して外部バスをロック状態とし、不揮発性メモリ８４に対するアクセスを不能にする。

【０１３２】

比較手段８２は、外部バスロック手段８１を実行した後に、ＦＬＡＧ記憶部７９の値が「１」であるかどうかをチェックし、ＦＬＡＧ記憶部７９内の値が「１」であれば、ＦＬＡＧ記憶部７９内に「０」を入れ、「１」を示す比較結果信号を外部バスロック解除手段８３に出力し、ＦＬＡＧ記憶部７９内の値が「１」でなければ、「０」を示す比較結果信号を外部バスロック解除手段８３に出力して処理を終了する。

【０１３３】

外部バスロック解除手段８３は、「１」を示す比較結果信号を比較手段８２から受けた場合には、外部バス制御部８５にロック解除信号を出力してカード６の外部バスのロクを解除し、また、「０」を示す比較結果信号を比較手段８２から受けた場合には、外部バス制御部８５にロック解除信号を出力せず、カード６の外部バスはロク状態のままとなる。

【０１３４】

不揮発性メモリ８４はＩＣカードやメモリカードなどのカード６にある保護すべきメモリ領域である。

【０１３５】

外部バス制御部８５はカード６の保護すべきメモリ領域と外部接続用Ｉ／Ｆとの間に設けたバス制御部である。

【０１３６】

ここで、電子印鑑５側の秘密鍵Ｋｓは、カード６側の公開鍵Ｋｐと論理的に関連しており、以下の各種暗号化方式により公開鍵Ｋｐと秘密鍵Ｋｓとは所定の鍵ペアを構成している。

（暗号化方式：ＲＳＡ方式）

公開鍵Ｋｐと秘密鍵Ｋｓの鍵ペアにおいてＲＳＡ公開鍵暗号方式を採用する場合には、次のように鍵ペアＫｐ，Ｋｓを決める。

【０１３７】

ほぼサイズの等しい二つの異なる素数ｐとｑを用意し、次式でｎを計算する。

$n = p \times q$、$p \neq q$

ｐ－１とｑ－１の最小公倍数ｎ１を計算する。

$n1 = LCM(p-1, q-1)$　　（２）

ｎ１に素なｅを求める。

$GCD(e, n1) = 1$　　（３）

次に、ｄを求める。式（３）からｅ$^{-1}$が存在することが判る。

$d = e^{-1} \bmod n1$　　（４）

鍵ペアの範囲は１＜ｅ，ｄ＜ｎ１である。

【０１３８】

公開鍵Ｋｐは（ｅ，ｎ）、秘密鍵Ｋｓは（ｄ）である。

【０１３９】

現在の計算機の計算能力において、鍵長（ｎの２進ビットの長さ）は１５３６であれば、安全である。

（暗号化方式：楕円曲線暗号方式）

公開鍵Ｋｐと秘密鍵Ｋｓの鍵ペアにおいて楕円曲線暗号を採用する場合には、次のように鍵ペアＫｐ，Ｋｓを決める。

【０１４０】

素数ｐとして、１６０ビット長の２進素数をランダムに選ぶ。

【０１４１】

楕円曲線Ｅとして、式（５）の条件を満たすように、ａ，ｂを選び楕円曲線が決まる。

$(4a^3+27b^2 \neq 0 \bmod p)$　　（５）

生成元Ｇとして、楕円曲線の生成元を一つ選ぶ。

$G=(X_0, Y_0)$　　（６）

ランダムな自然数ａとして、式（７）で乱数を選んで、式（８）で楕円曲線の点Ｇの倍数Ａを求める。

$a \in \{1, 2, \cdot\cdot, \#E-1\}$　　（７）

$A=aG=(X_a, Y_a)$　　（８）

ここで、＃Ｅは楕円曲線の位数である。

【０１４２】

公開鍵として（Ｅ，ｐ，＃Ｅ，Ｇ，Ａ）、秘密鍵として（ａ）である。

【０１４３】

【表１】

暗号方式および鍵情報

暗号方式	識別番号	公開鍵　Kp	秘密鍵　Ks
RSA	1	e, n	d
楕円曲線	2	E, p, #E, G, A	a

上記公開鍵Ｋｐは、カード会社などのような関連組織に自由に利用してもらうことが便利である。一方、上記秘密鍵Ｋｓは、電位印鑑５の中に閉じ込められており、アクセスできないようになっているため、安全性を向上させることができる。

【０１４４】

上記構成により、以下、本実施形態１の事前認証システム１の動作を説明する。

【０１４５】

図１に示すように、まず、ステップＳ１０１において、交信要求ＩＤ記憶部５２に記憶された交信要求ＩＤを、電子印鑑５側に内蔵されたカードリーダ／カードライタ５Ａからカード６側に送信して、カード６に対して電子印鑑５との直接交信を要求する。

【０１４６】

次に、ステップＳ１０２では、カード６側において、電子印鑑５側から受信した交信要求ＩＤを交信要求ＩＤ記憶部７１内の交信要求ＩＤと比較し、その比較結果が一致しなければ（ＮＯ）、ステップＳ１０３で処理を終了し、また、その比較結果が一致すれば（ＹＥＳ）、ステップＳ１０４の処理に移行する。

【０１４７】

ステップＳ１０４では、乱数発生手段７３により乱数Ｄ１をランダムに生成して乱数記憶部７４に記憶する。

【０１４８】

ステップＳ１０５では、暗号化手段７６により記憶乱数Ｄ１を公開鍵Ｋｐに基づいて暗号化する。その暗号化された乱数Ｄ１を、カード６側の送受信・整流・ロジック回路６Ａから電子印鑑５側のカードリーダ／カードライタ５Ａに送信する。

【０１４９】

電子印鑑５側では、ステップＳ１０６において、受信された暗号化乱数Ｄ１を、復号手段５４により秘密鍵Ｋｓに基づいて復号する。これによって、復号化された乱数Ｄ２が得られる。

【０１５０】

ステップＳ１０７では、復号化された乱数Ｄ２を、暗号化手段５５により秘密鍵Ｋｓに基づいて暗号化する。この暗号化された乱数を、電子印鑑５側のカードリーダ／カードライタ５Ａからカード６側の送受信・整流・ロジック回路６Ａに送信する。

【０１５１】

カード６側では、ステップＳ１０８において、受信された暗号化乱数を、復号手段７７により公開鍵Ｋｐに基づいて復号する。これによって、復号化された乱

数Ｄ３が得られる。

【０１５２】

ステップＳ１０９では、ステップＳ１０４で生成した記憶乱数Ｄ１とステップＳ１０８で得た乱数Ｄ３との照合を行う。この照合結果が一致した場合（ＹＥＳ）には、ステップＳ１１０の処理に進み、事前承認が有効であると判断してＦＬＡＧ記憶部７９に「１」を設定し、本人であると認める。

【０１５３】

また、ステップＳ１０９での照合結果が不一致であれば（ＮＯ）、ステップＳ１１１の処理に進み、事前承認は無効であると判断してＦＬＡＧ記憶部７９に「０」を設定し、本人として認めない。

【０１５４】

以上の一連の事前認証処理後（ステップＳ１０１～Ｓ１１１）に、ステップＳ１２１において、ホストコンピュータ３は、入力装置３１からのユーザ入力によりカードアクセス要求を、カードリーダ／カードライタ４を介してカード６側の送受信・整流・ロジック回路６Ａに送信する。

【０１５５】

カード６側においては、外部バスロック手段８１が外部バスをアクセス不能状態にして、不揮発性メモリ８４に対してアクセスを不能にしている。このとき、ステップＳ１２２でＦＬＡＧ記憶部７９の値が「１」であるかどうかを比較手段７２がチェックし、その値が「１」でなければ（ＮＯ）、ステップＳ１２３で「アクセス禁止」と判断して外部バスのロック状態を維持し、その旨を送受信・整流・ロジック回路６Ａからカードリーダ／カードライタ４を介してホストコンピュータ３側に送信する。ホストコンピュータ３側では、ステップＳ１２４で「カード６のアクセス不能」を検出して処理を終了する。

【０１５６】

ステップＳ１２２においてＦＬＡＧ記憶部７９の値が「１」であれば（ＹＥＳ）、ステップＳ１２５でＦＬＡＧ記憶部７９の値を「０」にリセットした後に、ステップＳ１２６で「アクセス許可」と判断して外部バスのロック解除を行い、その旨を送受信・整流・ロジック回路６Ａからカードリーダ／カードライタ４を

介してホストコンピュータ３側に送信する。ホストコンピュータ３側では、ステップＳ１２７で「カード６のアクセス成功」を検出し、セキュリティ処理として本人であることが認められる。

【０１５７】

このような事前認証が成功した後に、ホストコンピュータ３と遠隔サーバ２とが交信可能となり、ユーザ選択実行処理後に遠隔サーバ２内の所望のカード関連情報を、サービス内容出力処理として画面表示させたりプリントアウトさせたりすることができる。

（実施形態２）

上記実施形態１では、事前認証方式の電子印鑑５およびカード６を含む基本構成として事前認証システム１について説明したが、本実施形態２では、より機能の豊かな事前認証方式のマルチモード電子印鑑およびマルチモードカードを含む応用構成としてのマルチモード事前認証システムについて説明する。

【０１５８】

図７は、本発明の実施形態２におけるマルチモード事前認証システムの要部構成を示すブロック図である。

【０１５９】

図７において、このマルチモード事前認証システム１０は、遠隔サーバ２と、ホストコンピュータ３（またはパーソナルコンピュータ；以下パソコンという）と、カードとの交信インターフェースであるリーダー・ライター装置としてのカードリーダ／カードライタ４と、マルチモード電子印鑑７と、リムーバブルメモリ媒体としてのＩＣカードやメモリカードなどのマルチモードカード９とを備えている。

【０１６０】

なお、このマルチモード事前認証システム１０において、上記実施形態１の事前認証システム１と異なるのは、後述する図８および図９のマルチモード電子印鑑７および図１０および図１１のマルチモードカード９のように各マルチモード部が追加されている点であって、前述した遠隔サーバ２、ホストコンピュータ３（またはパーソナルコンピュータ；以下パソコンという）およびカードリーダ／

カードライタ４，７Ａの各構成部材の作用効果については上記実施形態１の場合と同様であるので、ここではその詳細な説明を省略する。

【０１６１】

マルチモード電子印鑑７は、図７に示すように、カードリーダ／カードライタ７Ａと、セキュリティ処理部７Ｂ（事前認証モード部７３）を含むマルチモード部とを有している。

【０１６２】

図８は、本発明の実施形態２におけるマルチモード事前認証システムのマルチモード電子印鑑の要部構成例を示すブロック図であり、図９は、図８のマルチモード電子印鑑の外観構成例を示す斜視図である。

【０１６３】

図８および図９において、マルチモード電子印鑑７は、マルチモード部として、初期設定モード部７１と、届印モード部７２と、事前承認モード部７３と、取り消しモード部７４と、時計モード部７５と、期間設定モード部７６と、回数設定モード部７７と、金額設定モード部７８と、時計設定モード部７９と、ＬＣＤ表示部８０と、選択キー８１と、決定キー８２と、カウンタキー８３と、スタートキー８４とを有している。

【０１６４】

初期設定モード部７１は、電子印鑑７の鍵情報（公開鍵、秘密鍵などの情報）を外部から入力して設定する。この初期設定モード部７１内の鍵情報記憶部（図示せず）への鍵情報の初期設定は、鍵管理センターや電気屋などで初期設定用の専用機器を使って行うようにすればよい。この初期設定が未実行の場合には鍵情報記憶部（図示せず）の記憶情報がオール「１」であるように設定し、このときのみ、鍵情報記憶部に対して鍵情報の初期設定処理を実行できるように構成する。即ち、初期登録に際して、登録許可レジスタが特定のデータ配列の時にのみ、鍵情報の暗号鍵データを入力できる構成になっている。その設定結果は、設定結果画面として初期設定モードの実行完了を示す「ＯＫ」または、初期設定不能を示す「ＮＧ」がＬＣＤ表示部８０上に表示され、これによってユーザに報知されるようにする。この制御は、図２に示すカードリーダ／カードライタ７Ａにおけ

る制御回路４６内のＣＰＵが介入し、選択キー８１を使ってＬＣＤ表示部８０上で各種モード表示から初期設定モードを選び、決定キー８２のキー操作によって所望のモード、即ち初期設定モードを決定する。その後に、スタートキー８４を押し続け、選択された初期設定モードが実行されてＬＣＤ表示部８０上に「ＯＫ」また「ＮＧ」が表示されたらスタートキー８４を放せば初期設定モードが終了するようになっている。

【０１６５】

届印モード部７２は、初期設定モード部７１によって電子印鑑７内に格納している公開鍵を、後述するマルチモードカード９側に出力させて届印処理する。この届印モード部７２の選択、決定、実行（スタート）、実行結果の表示確認は初期設定モード部７１における上記一連の動作手順の場合と同じである。

【０１６６】

事前承認モード部７３は、後述するマルチモードカード９に対して事前承認処理を行う。この事前認証処理と同時に、設定した期間・回数・金額の内容をカード９側に伝送する。カード９がメモリカードの場合に、メモリカードでは金額に関する内容がないので、メモリカードが受信した金額の内容が無視される。この事前承認モードの選択（選択キー８１）、決定（決定キー８２）、実行（スタートキー８４）、ＬＣＤ表示部８０の実行結果画面の表示確認は初期設定モード部７１における上記一連の動作手順の場合と同じである。

【０１６７】

取り消しモード部７４は、上記事前承認結果を取り消すためのものである。この取り消しモードの選択、決定、実行、実行結果の表示確認は初期設定モード部７１における上記一連の動作手順の場合と同じである。

【０１６８】

時計モード部７５は、年月日時刻などの時情報をＬＣＤ表示部８０上で表示するモードである。電子印鑑７は特定操作がなければ、この時計モード部７５による時計モードが自動的に選択されて、年月日時刻が表示画面上に表示されるようになっている。

【０１６９】

期間設定モード部７６は、設定した日数を時計モード部７５による日時と足し合わせてカード９側に送信するように動作するモードである。即ち、期間設定モード部７６は有効期間（日数）の数値をカウンターキー８３から入力し、その入力数値を関連メモリに記憶する。この登録データの書き換えは繰り返しできる。この期間設定モードは、選択キー８１を使って各種モードから選択され、決定キー８２を使って所望のモードに決定する。それから数字（日時）の設定はカウンタキー８３を使ってＬＣＤ表示部８０上で画面に表示された値を見ながら行うことができる。設定した数字（日時）を関連メモリ（例えば図２のカードリーダ／カードライタ５Ａにおける不揮発性メモリ４４など）に記憶する。このモードの実行は電子印鑑７以外の機器に関係ないので、変調回路４１と復調回路４２を止めてもよい。

【０１７０】

回数設定モード部７７は、事前承認１回でカード９の使える有効使用回数を関連メモリに設定する。この登録データの書き換えは繰り返しできる。その設定方法は期間設定モード部７６の場合と同じである。

【０１７１】

金額設定モード部７８は、ＩＣカードに１回に使える金額の上限値を設定することができる。この登録データの書き換えは繰り返しできる。この設定方法も期間設定モード部７６の場合と同じである。

【０１７２】

時計設定モード部７９は、年月日時間を合わせるためのモードである。この設定方法も期間設定モード部７６の場合と同じである。

【０１７３】

ＬＣＤ表示部８０は、各種モードを表示する初期画面である設定メニュ画面、各種モードの実行結果を表示する実行結果画面などを表示可能である。ＬＣＤ表示部８０を表示駆動するドライバ（図示せず）は、図２のカードリーダ／カードライタ７Ａにおける制御回路４６に組み込まれている。

【０１７４】

選択キー８１は制御回路４６のＣＰＵを通してモードを選択する。

【０１７５】

決定キー８２は制御回路４６のＣＰＵを通して選択したいモードを決定する。

【０１７６】

カウンタキー８３は制御回路４６のＣＰＵを通して選択決定モードに数字設定があればこのキーを使って数字を設定する。

【０１７７】

スタートキー８４は制御回路４６のＣＰＵを通してその押圧動作により実行を開始する。この場合、初期設定モード部７１、届印モード部７２、事前承認モード部７３、取り消しモード部７４の四つのモードを実行する。その押圧動作を止めるとモードが終了する。

【０１７８】

以上のように、マルチモード電子印鑑７側に表２のマルチモードを設ける。

【０１７９】

【表２】

電子印鑑のモード一覧表

モード	操作キー	処理内容	関連機器	確認方法
初期設定	選択、決定	鍵情報の登録	専用機器	LCD(OK, NG)
届印	選択、決定	公開鍵の出力	カード	LCD(OK, NG)
事前承認	選択、決定	承認と承認内容の出力	カード	LCD(OK, NG)
取り消し	選択、決定	承認の取り消し	カード	LCD(OK, NG)
期間設定	選択、決定、カウンタ	設定内容記録	なし	LCD(内容)
回数設定	選択、決定、カウンタ	設定内容記録	なし	LCD(内容)
金額設定	選択、決定、カウンタ	設定内容記録	なし	LCD(内容)
時計設定	選択、決定、カウンタ	時計の時間合わせ	なし	LCD(内容)

マルチモードカード９は、図７に示すように、図４の送受信・整流・ロジック回路９Ａと、図１０のセキュリティ処理部９Ｂを含むマルチモード部と、図１１のアクセス許可処理部９Ｃとを有している。

【０１８０】

図１０は、図７のマルチモードカード９におけるマルチモード部９Ｂの要部構

成例を示すブロック図である。

【０１８１】

図１０において、マルチモード部は、初期設定モード部９０と、事前認証モード部９１と、取り消しモード部９２と、期間設定モード部９３と、回数設定モード部９４と、金額設定モード部９５とを有している。

【０１８２】

初期設定モード部９０は、マルチモード電子印鑑７内の公開鍵を出力して生カード内に登録するための処理を行う。この処理はユーザ本人が行うことができる。例えばカード９を発行して貰うときに、身元確認のために電子印鑑７を届印として渡して、登録してもらうことも考えられる。同じカード９に対してこのモードを１回しか実行できないように構成している。このモードは電子印鑑７から受信した届印モードのＩＤ番号より識別される。カード９側が設定の結果「ＯＫ」または「ＮＧ」を電子印鑑７側に送信し、電子印鑑７側のＬＣＤ表示部８０上にこれを表示するようになっている。

【０１８３】

事前認証モード部９１は前述したような事前認証処理を行う。電子印鑑７との交信によりカード９の事前承認を許可または拒否する。このモードは電子印鑑７から受信した承認モードのＩＤ番号より識別される。カード９側が承認の結果「ＯＫ」または「ＮＧ」を電子印鑑７側に送信し、電子印鑑７側のＬＣＤ表示部８０上にこれを表示する。

【０１８４】

取り消しモード部９２は認証済みカード９に対して事前認証結果を取り消すためのモードである。まず、事前認証モード部９１による事前認証処理を実行する。事前承認の結果が「ＯＫ」であれば、電子印鑑７が本物であり、事前承認を取り消し、「ＯＫ」を電子印鑑７側に送る。事前承認の結果が「ＮＧ」であれば、電子印鑑７は本物でなく、カード９の事前承認状態をそのまま維持し、「ＮＧ」を電子印鑑７側に送る。このモードは事前承認していないカード９に対しても、正しく実行できる。確実に事前認証を無効にするときに、このモードを実行すればよい。

【０１８５】

以上のマルチモードカード９側に表３のマルチモードを設ける。

【０１８６】

【表３】

カードのモード一覧表

モード	識別方法	処理内容	関連機器	確認方法
初期設定	印鑑側の届印モード	公開鍵の登録	電子印鑑	電子印鑑側
事前承認	印鑑側の承認モード	承認と承認内容の記録	電子印鑑	電子印鑑側
取り消し	印鑑側の取り消しモード	承認の取消	電子印鑑	電子印鑑側

図１１は、図７のマルチモードカード９におけるアクセス許可処理部９Ｃの要部構成例を示すブロック図である。

【０１８７】

図１１において、アクセス許可処理部９Ｃは、外部バスロック手段９６と、ＦＬＡＧ記憶部７９と、期間記憶部９７と、カウントダウン・回数記憶部９８と、比較手段９９と、外部バスロック解除手段１００と、不揮発性メモリ１０１と、外部バス制御部１０２とを有している。

【０１８８】

外部バスロック手段９６は、外部バスをアクセス（書き込みまたは読み出し動作）不能にする。ホストコンピュータ３（または汎用パーソナルコンピュータ）からカードリーダ／ライタ４さらに送受信・整流・ロジック回路９Ａを経由して、不揮発性メモリ１０１にアクセスしようとするときに、送受信・整流・ロジック回路９Ａのパワーオンリセット回路６６からの信号をトリガーとしてカード９の外部バス制御部１０２をロック状態にし、不揮発性メモリ１０１へのアクセスを不能にする。

【０１８９】

期間記憶部９７は有効期間を記憶するものである。

【０１９０】

カウントダウン・回数記憶部９８は回数記憶部（関連メモリ；図示せず）に記憶している値から１を引き、その結果を回数記憶部に再度記憶する。図４のパワ

ーオンリセット回路６６の信号をトリガーとしてこの処理を行う。

【０１９１】

比較手段９９は、外部バスロック手段９６によるバスロック処理を実行後に、ＦＬＡＧ記憶部７９、期間記憶部９７、カウントダウン・回数記憶部９８の各値をチェックし、ＦＬＡＧ記憶部７９の値が「１」であれば、比較処理を継続する。期間記憶部９７の値がホストコンピュータ３（または汎用パーソナルコンピュータ）から得た年月日時間と比較し、有効使用期間内であれば処理を継続する。カウントダウン・回数記憶部９８の値をチェックし、正であれば外部バスロック手段９５によるバスロック処理を実行する。ＦＬＡＧ記憶部７９の値が「０」であれば、処理を終了する。有効使用期間切れまたは回数記憶部の値が負であれば、ＦＬＡＧ記憶部９６に「０」を書く込んで処理を終了する。

【０１９２】

外部バスロック解除手段１００は、カード９の外部バスのロックを解除する。

【０１９３】

不揮発性メモリ１０１はＩＣカードまたはメモリカードなどカード９にある保護すべきメモリ領域である。

【０１９４】

カード９の外部バス制御部１０３はカードの保護すべきメモリ領域（不揮発性メモリ１０１）と外部接続用Ｉ／Ｆとの間に設けたバス制御部である。

【０１９５】

金額記憶部１０３は、１回に使える金額の上限値を記憶する。なお、金額記憶部１０３があるのはＩＣカードだけでありメモリカードにはこの記憶部はない。

【０１９６】

比較手段１０４は、不揮発性メモリ１０１から呼び出される金額の値を監視し、金額記憶部１０３の値を超えたら、カード９の外部バスをロック状態とし、カード９を使用不能にする。なお、比較手段１０４があるのはＩＣカードだけでありメモリカードにはこの比較手段１０４が存在しない。

【０１９７】

以上により、本実施形態１，２によれば、電子印鑑５または７側からカード６

または９に対して交信要求（ＩＤ）を送信し、カード６または９はこれをチェックする。チェックがＯＫであれば、カード６または９の事前認証部のカードセキュリティ処理部６Ｂまたは９Ｂでは、ランダム乱数を発生させ、これを公開鍵で暗号化して、電子印鑑５または７側に送り、電子印鑑５または７はこの受け取ったデータを秘密鍵で復号化し、さらに秘密鍵で暗号化してカード６または９に送る。このデータを受け取ったカード６または９は、又公開鍵で復号化する。このようにして、事前に本人認証を終えたカード６または９は、一度だけホストコンピュータを介して遠隔サーバ２と交信できる。即ち一度だけなら、カード使用時点で事前の本人認証をせずにカード６または９をそのまま使用できる。以後このカード６または９は、使用の度に事前承認手続きをしておけばよく、電子印鑑５または７を持ち運ぶ必要がない。したがって、電子印鑑５または７にカード会社のＩＤ番号を組み込むこともなく、電子印鑑５または７を届印としてカード６または９に登録してカード６または９を容易に発行でき、かつ、従来の電子印鑑５または７を用いないシステムに対して新たなる改造や増設をすることなく、処理相手に電子印鑑５または７を渡さずに、電子印鑑５または７を高セキュリティでカード６または９のアクセス保護に使用することができる。

【０１９８】

なお、上記実施形態１，２の電子印鑑５または７の応用可能な分野を図１２に示している。図１２における括弧の中の内容は、従来の本人認証方法を示している。

【０１９９】

従来では、例えば、カードによる買い物を行う場合などには、署名を目視確認することにより本人認証が行われている。また、カードによる現金引き出し、携帯電話装置などによる遠隔家電制御、カードによる携帯電話装置などの課金、パーソナルコンピュータへのアクセス、電子錠の開錠を行う場合などには、暗証番号を入力することにより本人認証が行われている。また、入退室管理、給油・高速料の支払い、電車の乗車料金・公衆電話料金の支払いを行う場合などには、カードを確認することによって本人認証が行われており、カードの所持者は真性な利用者であると判断されている。また、車両防犯のためには、車両の鍵によって

本人認証が行われており、鍵の保持者は車両の真性な利用者であると判断されている。また、市役所の窓口などでは、伝統印鑑により本人認証が行われており、書き留め郵便配達の受け取りでは、伝統印鑑またはサインにより本人認証が行われている。また、高級家電の盗難防止については、個人が管理しているだけであり、本人認証による使用許可などは行われていない。

【０２００】

このような分野で、本発明の電子印鑑５または７を従来の認証方法と組み合わせて用いることによって、利用者に負担をかけずに、安全性を格段に向上させることができる。暗証番号は、盗難にあっても被害が発生しない限り発覚されないが、本発明の電子印鑑５または７は盗難にあったときに気が付き易く、被害防止対策を早急に行うことができる。また、電子印鑑５または７を紛失しただけでは、被害は生じにくい。

【０２０１】

従来は、市役所の窓口などでの本人認証、書き留め郵便配達の受け取りには、伝統印鑑が用いられているが、今後、例えば国民総背番号制などのように、個人情報が電子データ化され、そのデータを利用して情報・サービスが提供されると共に個人の権利・義務が管理されるような、いわゆる電子化政府になっていくことを考えると、本発明の電子印鑑５または７を伝統印鑑に変えて利用することは、非常に有効である。

【０２０２】

また、高級家電製品などに本人認証機能を加えることによって、盗難を防止することができる。テレビジョンセット、冷蔵庫、ビデオ、カメラなどの電子機器に対して、本発明の電子印鑑５または７による本人認証機能を設けて、電源投入の際に本人認証を要求することによって、本発明の電子印鑑５または７が無いと、これらの電子機器が作動しないことになる。このような機能は、発展途上国において実効性がある。

【０２０３】

さらに、定期券などのＩＣカードにおいて、本発明の電子印鑑５または７による本人認証機能を設けることによって、ＩＣカードを紛失した場合の届率が高く

なると考えられる。

【０２０４】

特に、本発明の電子印鑑５または７を携帯電話装置に着脱自在に搭載し、本発明の電子印鑑５または７が携帯電話装置のインターフェースを共用するように構成することもできる。携帯電話装置の機種変更時に本発明の電子印鑑５または７を取り除いて、新たな機種の携帯電話装置の機種変更時に本発明の電子印鑑５または７を容易に取り付けることができるようにする。また、本発明の電子印鑑５または７の形状は電池のような円柱形状や角柱形状の他、カード形状であってもよい。

【０２０５】

また、車の盗難防止対策としても本発明の電子印鑑５または７を用いることができる。この場合に、本発明の電子印鑑５または７を車のキーと同様に用い、本発明のカード６または９の事前認証処理部のセキュリティ処理部６Ｂまたは９Ｂおよびアクセス許可処理部６Ｃまたは９Ｃと、ホストコンピュータ３の各機能を車の制御部内に車両始動制御装置として搭載するようにしてもよい。

【０２０６】

【発明の効果】

以上のように、本発明によれば、カードに製造段階で電子印鑑により事前承認に関する機能を持たせることができる。

【０２０７】

また、電子印鑑を用いてカードで事前認証を行うため、従来のようにカードと電子印鑑を一緒に提出する必要がなく、カード使用時に、事前承認済みのカードだけを提出すればよいため、ユーザに負担かけることがなく、カードのデータを確実に保護することができる。

【０２０８】

さらに、事前認証機能のあるカードは従来のシステム上に事前認証機能の無いカードと同様に使えるため、従来のシステムを新たに改造せずとも、そのまま使用することができる。

【図面の簡単な説明】

【図１】

本発明の事前認証システムの実施形態１における要部構成を示すブロック図である。

【図２】

図１のカードリーダ／カードライタ４の要部構成例を示すブロック図である。

【図３】

図１の電子印鑑５におけるセキュリティ処理部５Ｂの要部構成例を示すブロック図である。

【図４】

図１のカード６に内蔵する送受信・整流・ロジック回路６Ａの要部構成例を示すブロック図である。

【図５】

図１のカード６におけるセキュリティ処理部６Ｂの要部構成例を示すブロック図である。

【図６】

図１のカード６におけるアクセス許可処理部６Ｃの要部構成例を示すブロック図である。

【図７】

本発明の実施形態２におけるマルチモード事前認証システムの要部構成を示すブロック図である。

【図８】

本発明の実施形態２におけるマルチモード事前認証システムのマルチモード電子印鑑の要部構成例を示すブロック図である。

【図９】

図８のマルチモード電子印鑑の外観構成例を示す斜視図である。

【図１０】

図７のマルチモードカード９におけるマルチモード部９Ｂの要部構成例を示すブロック図である。

【図１１】

図７のマルチモードカード９におけるアクセス許可処理部９Ｃの要部構成例を示すブロック図である。

【図１２】

本発明の電子印鑑の応用可能な分野を示す図である。

【図１３】

従来の本人認証システムの一例を示すブロック図である。

【図１４】

本発明者らが関連特許出願で提案した本人認証システムの一実施形態における要部構成を示すブロック図である。

【図１５】

図１４の本人認証システム２００において電子印鑑により本人認証を行う際に、ＩＣカードと電子印鑑との間に発生する処理内容を示すフローチャートである。

【符号の説明】

１　事前認証システム

２　遠隔サーバ

３　ホストコンピュータ

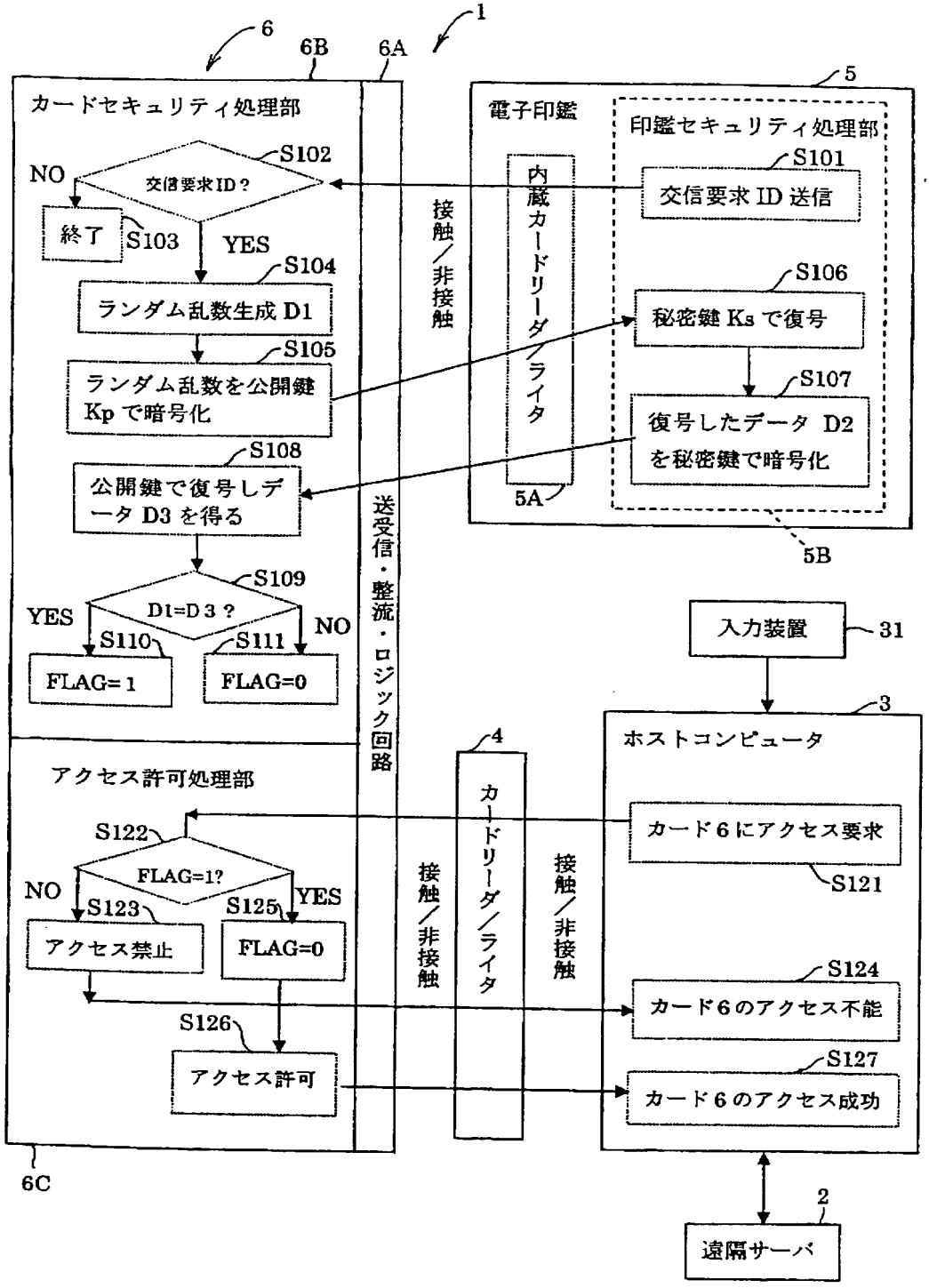
４，５Ａ，７Ａ　カードリーダ／カードライタ

５，７　電子印鑑

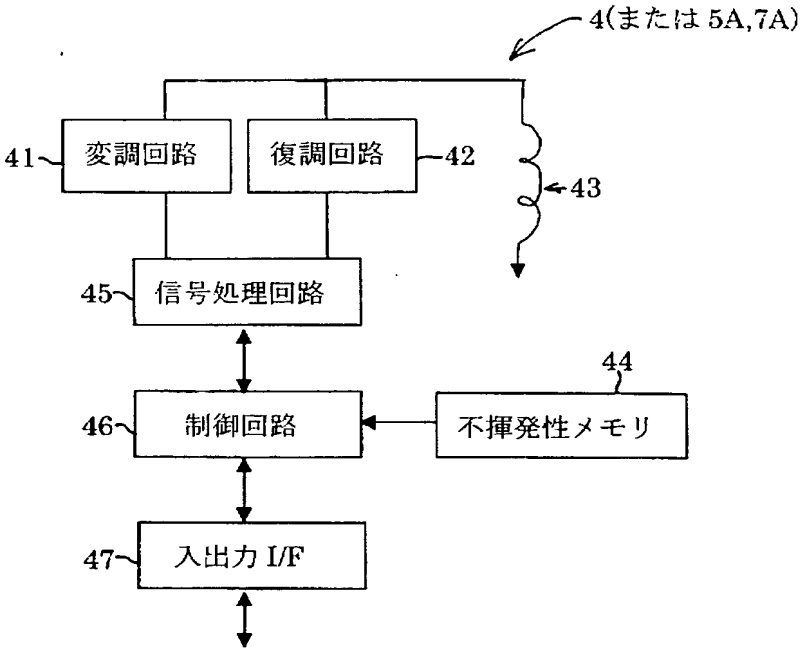
６，９　カード

【書類名】　図面

【図１】

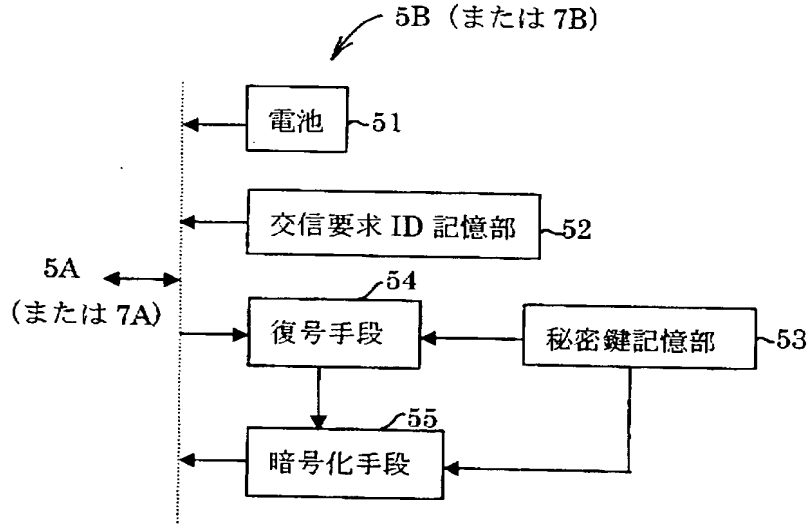

1
6
6B
6A
カードセキュリティ処理部
S102
交信要求ID？
NO
終了
S103
YES
S104
ランダム乱数生成 D1
S105
ランダム乱数を公開鍵 Kp で暗号化
S108
公開鍵で復号しデータ D3 を得る
S109
D1=D3？
YES
NO
S110
FLAG=1
S111
FLAG=0
アクセス許可処理部
S122
FLAG=1?
NO
YES
S123
アクセス禁止
S125
FLAG=0
S126
アクセス許可
6C
接触／非接触
送受信・整流・ロジック回路
5
電子印鑑
印鑑セキュリティ処理部
S101
交信要求 ID 送信
内蔵カードリーダ／ライタ
S106
秘密鍵 Ks で復号
S107
復号したデータ D2 を秘密鍵で暗号化
5A
5B
入力装置
31
3
ホストコンピュータ
4
カードリーダ／ライタ
接触／非接触
接触／非接触
カード６にアクセス要求
S121
S124
カード６のアクセス不能
S127
カード６のアクセス成功
2
遠隔サーバ

【図２】

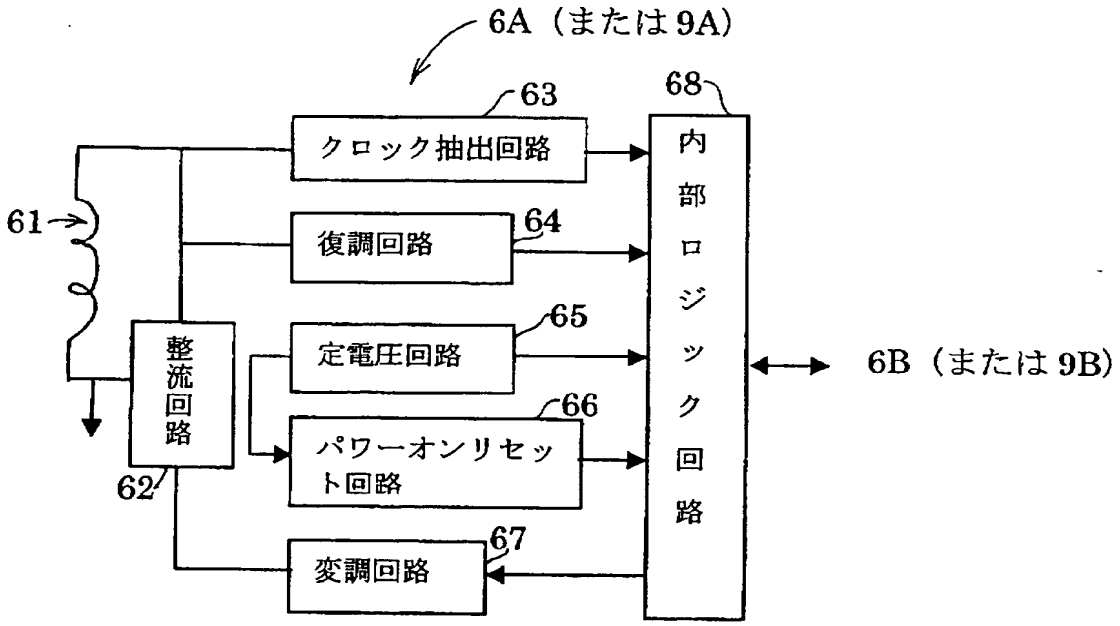


ホストコンピュータ 3 または電子印鑑 5

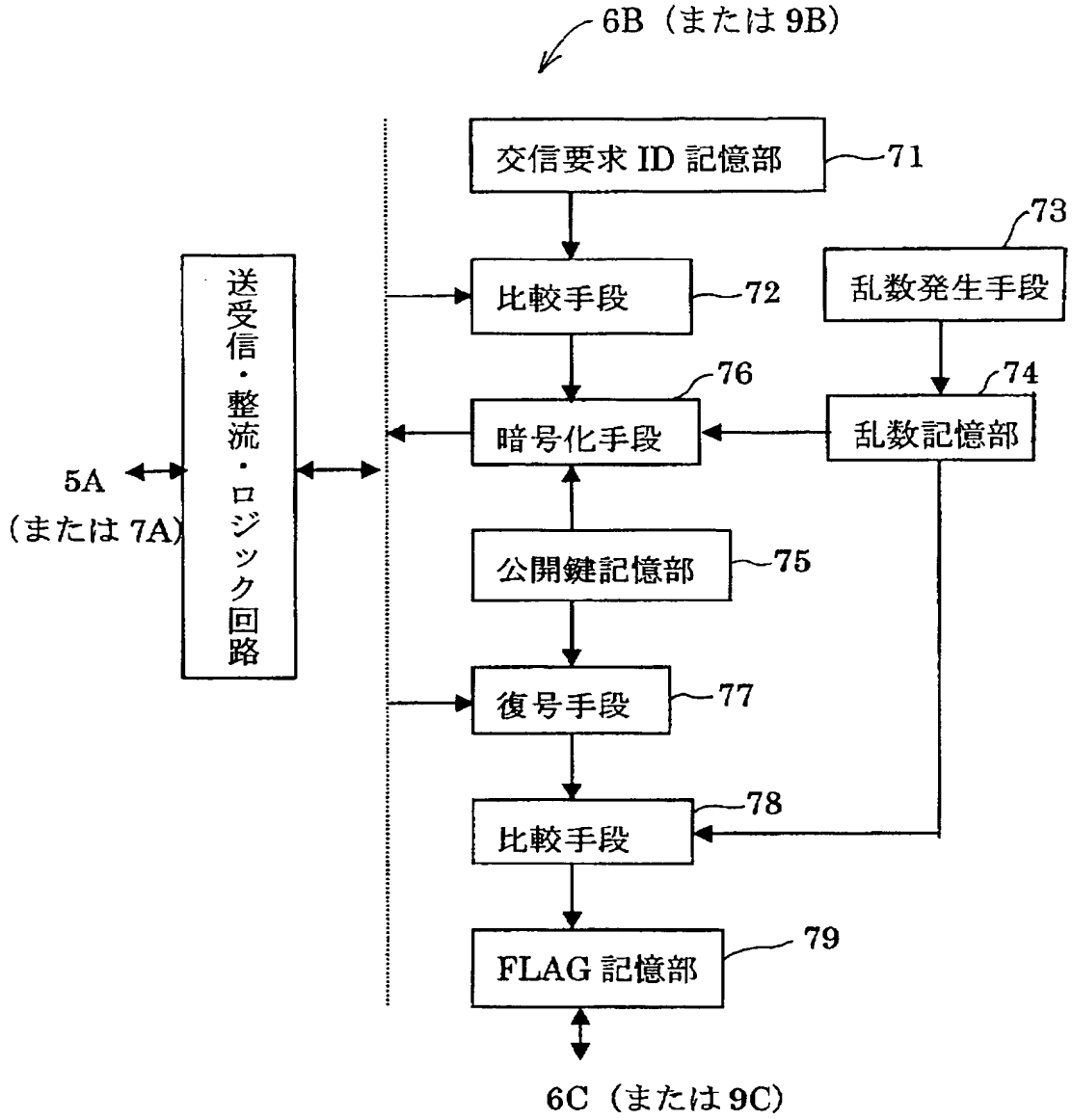
【図３】



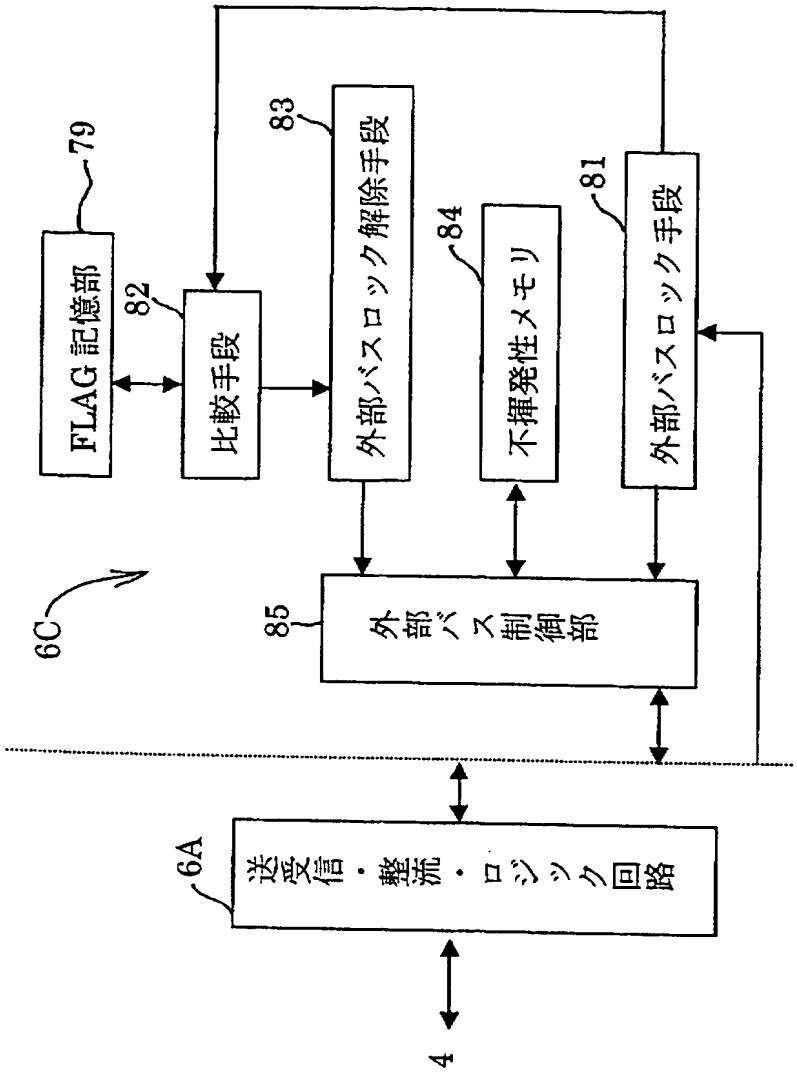
【図４】


6A（または9A）
63
68
クロック抽出回路
内部ロジック回路
61
復調回路
64
65
整流回路
定電圧回路
6B（または9B）
66
パワーオンリセット回路
62
67
変調回路

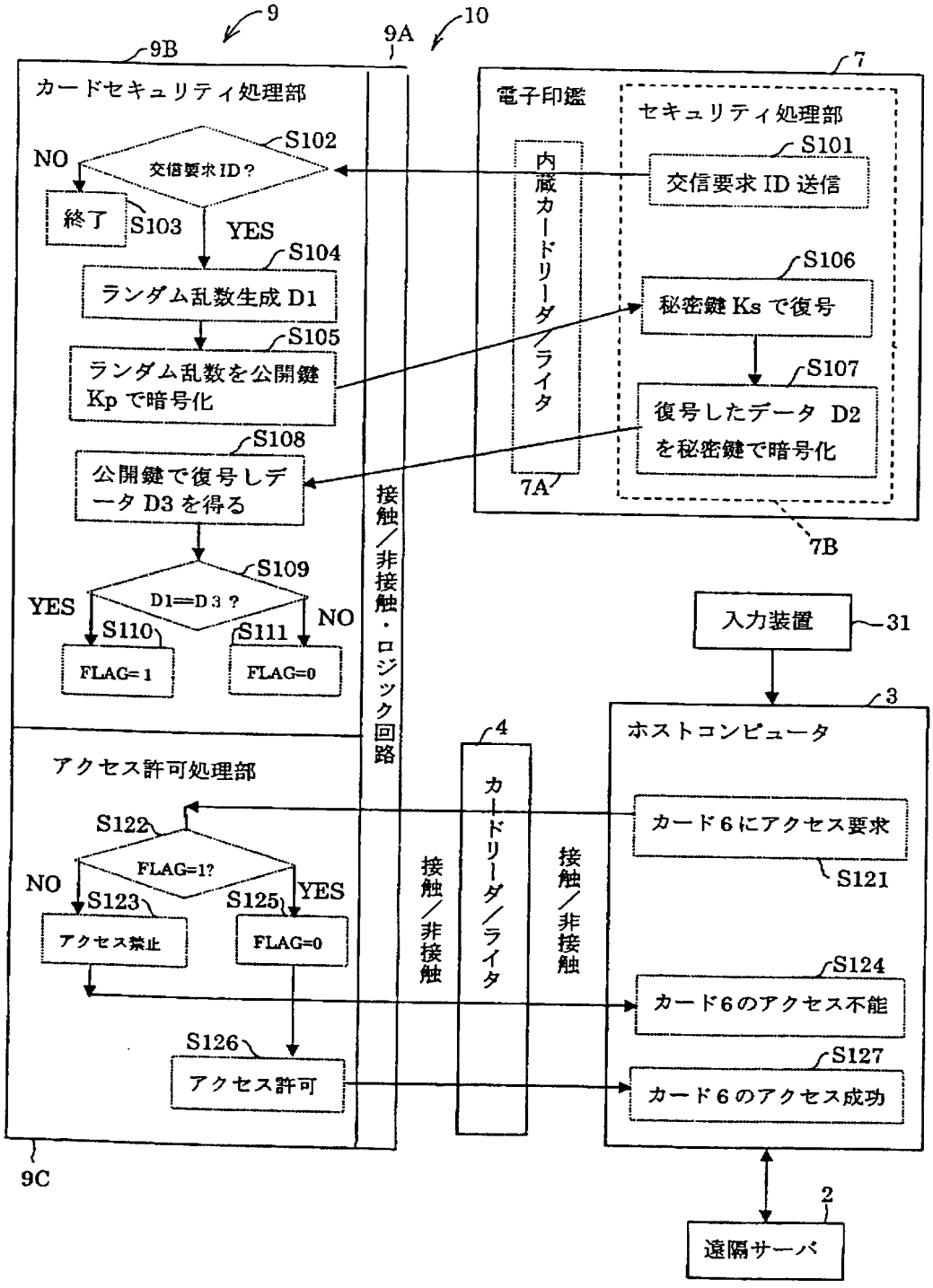
【図５】


6B（または9B）
交信要求ID記憶部
71
73
乱数発生手段
比較手段
72
76
74
暗号化手段
乱数記憶部
5A
（または7A）
送受信・整流・ロジック回路
公開鍵記憶部
75
復号手段
77
78
比較手段
FLAG記憶部
79
6C（または9C）

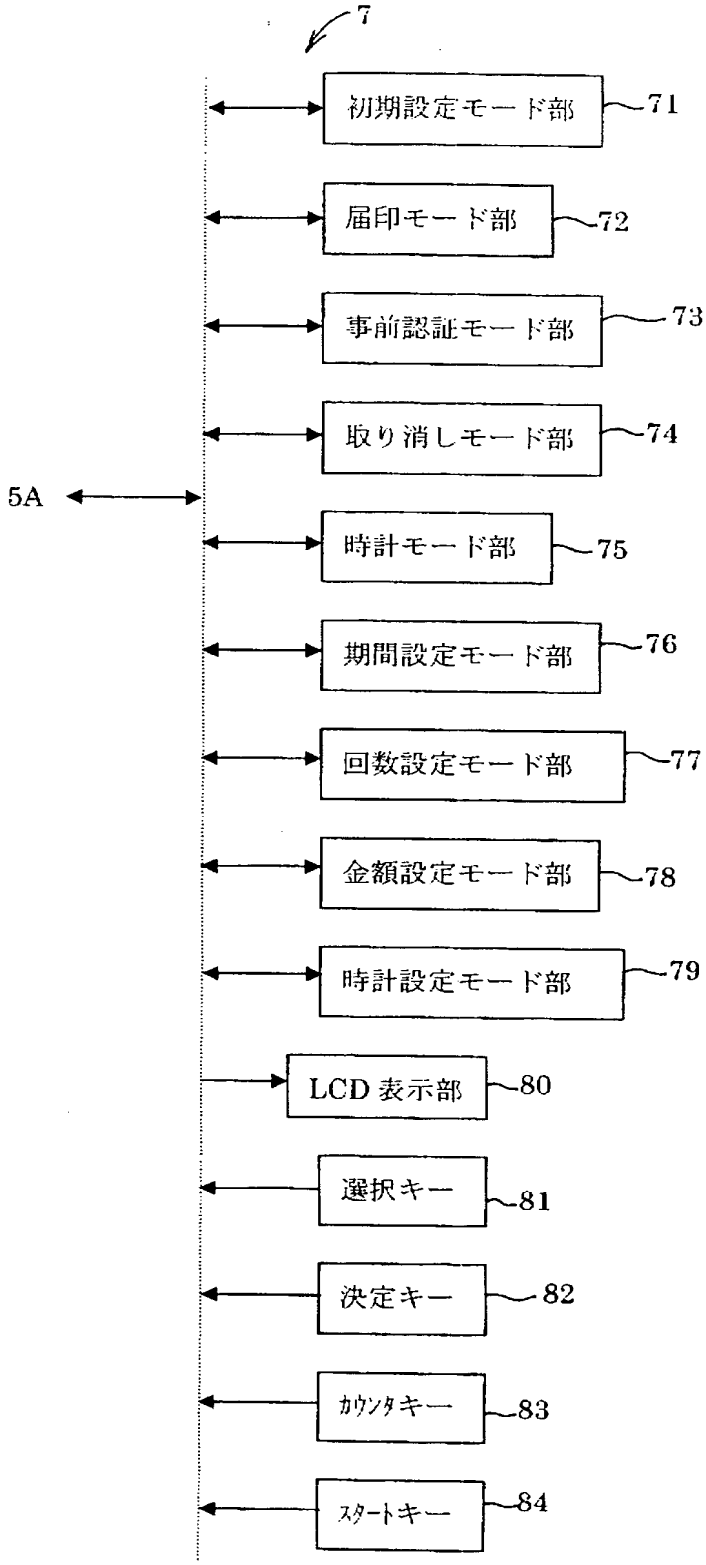
【図６】


79
FLAG 記憶部
82
比較手段
83
外部バスロック解除手段
84
不揮発性メモリ
81
外部バスロック手段
6C
85
外部バス制御部
6A
送受信・整流・ロジック回路
4

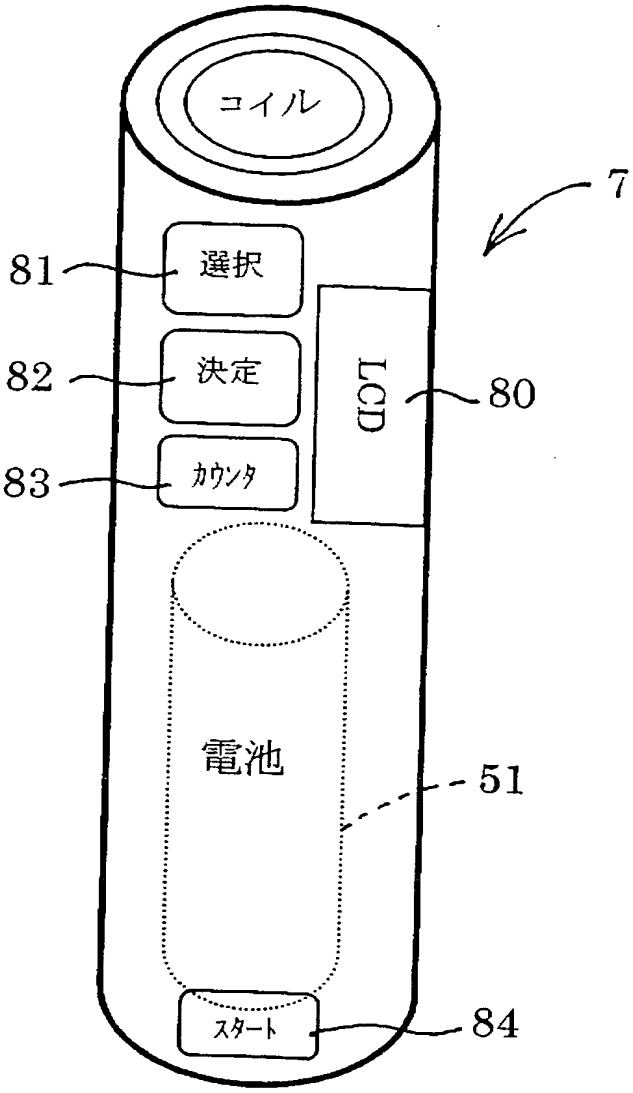
【図７】


9
10
9A
9B
カードセキュリティ処理部
電子印鑑
セキュリティ処理部
7
S102
交信要求ID？
NO
終了
S103
YES
S104
ランダム乱数生成 D1
S105
ランダム乱数を公開鍵 Kp で暗号化
S108
公開鍵で復号しデータ D3 を得る
S109
D1=D3？
YES
NO
S110
FLAG=1
S111
FLAG=0
S101
交信要求 ID 送信
S106
秘密鍵 Ks で復号
S107
復号したデータ D2 を秘密鍵で暗号化
内蔵カードリーダ／ライタ
7A
7B
接触／非接触・ロジック回路
入力装置
31
3
ホストコンピュータ
4
カードリーダ／ライタ
アクセス許可処理部
S122
FLAG=1?
NO
S123
アクセス禁止
S125
YES
FLAG=0
S126
アクセス許可
接触／非接触
接触／非接触
カード６にアクセス要求
S121
S124
カード６のアクセス不能
S127
カード６のアクセス成功
9C
2
遠隔サーバ

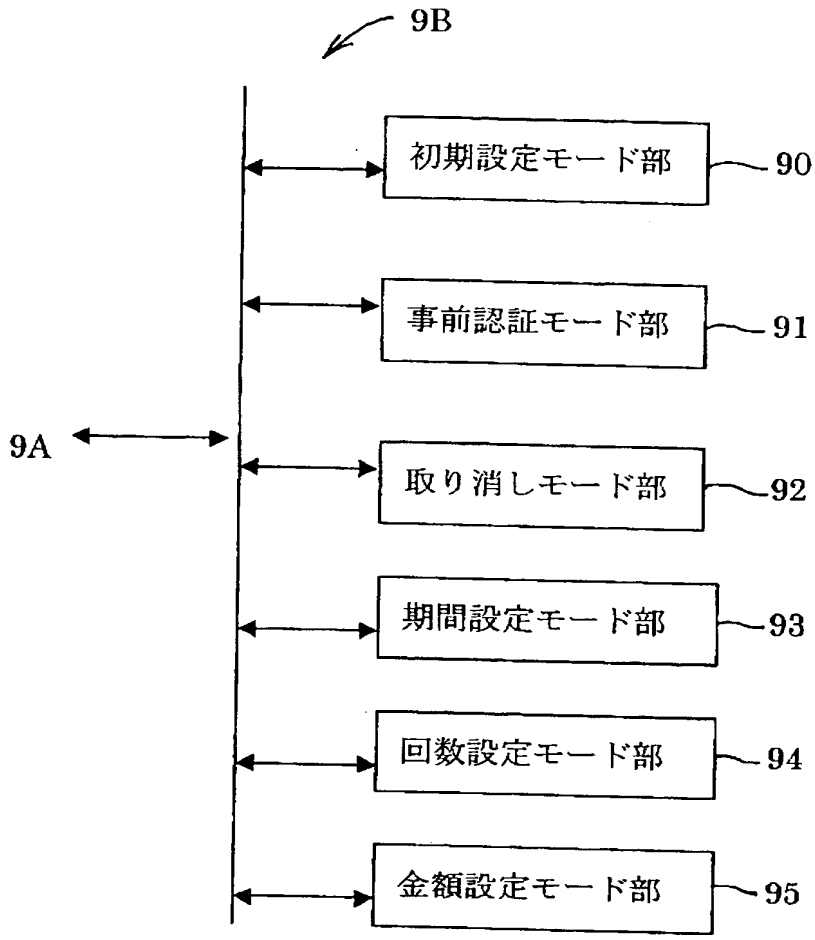
【図８】


7
初期設定モード部
71
届印モード部
72
事前認証モード部
73
取り消しモード部
74
5A
時計モード部
75
期間設定モード部
76
回数設定モード部
77
金額設定モード部
78
時計設定モード部
79
LCD 表示部
80
選択キー
81
決定キー
82
ｶｳﾝﾀｷｰ
83
ｽﾀｰﾄｷｰ
84

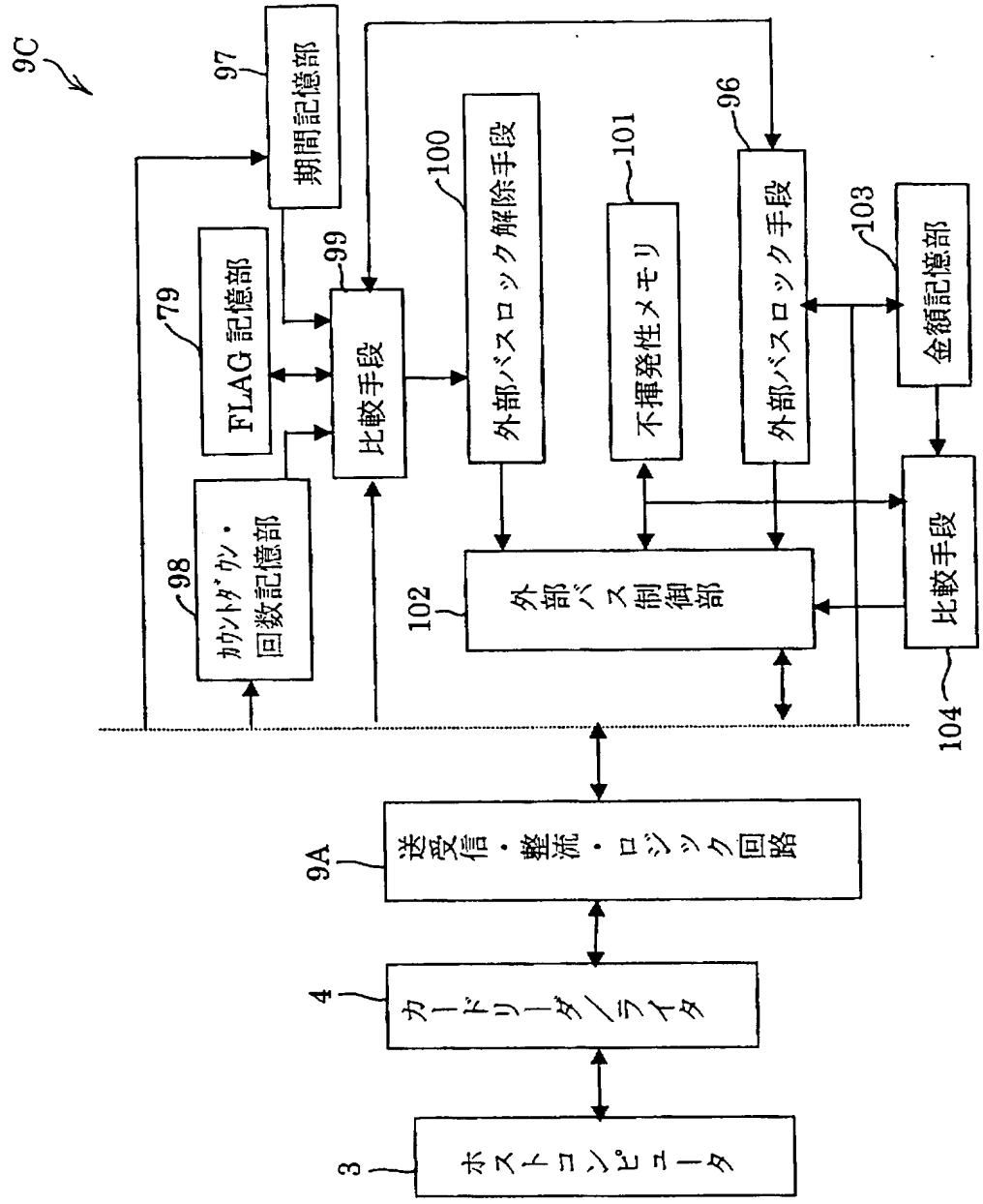
【図９】



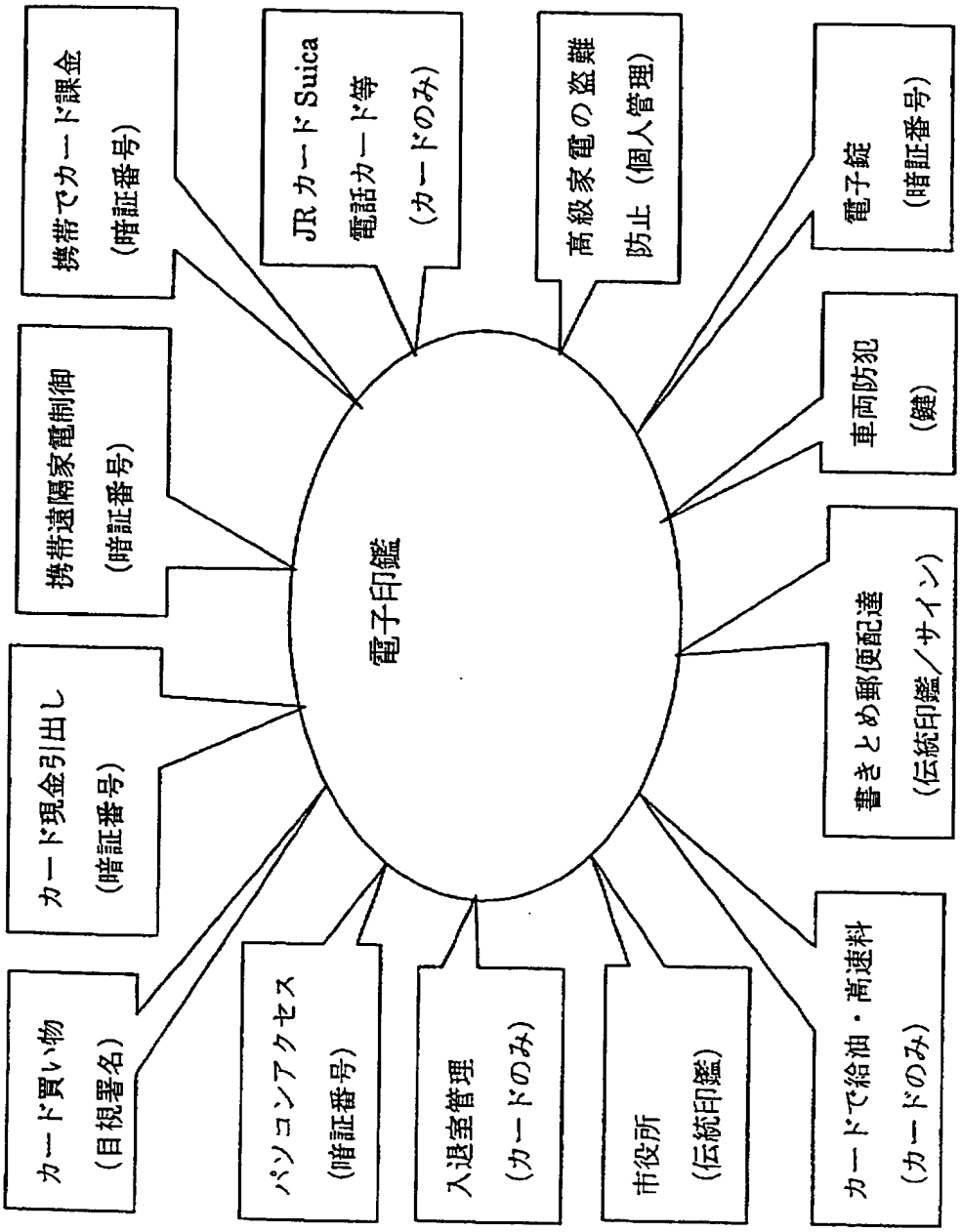
【図１０】


9B
初期設定モード部
90
事前認証モード部
91
9A
取り消しモード部
92
期間設定モード部
93
回数設定モード部
94
金額設定モード部
95

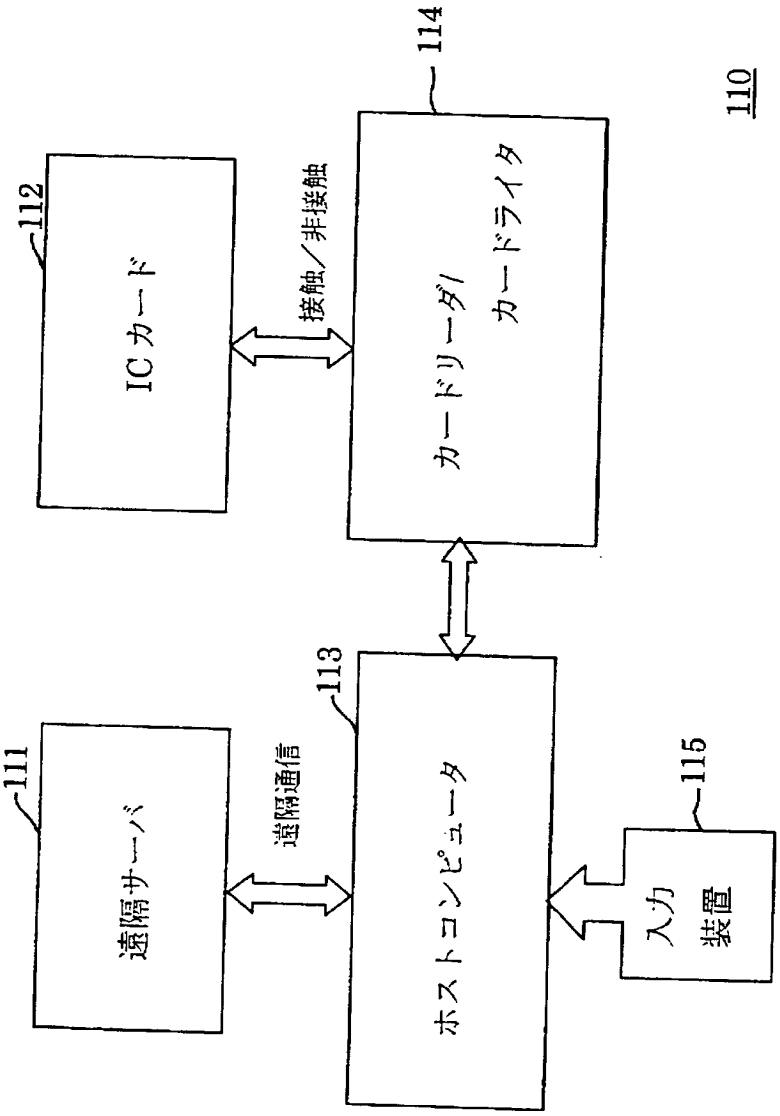
【図１１】


9C
97
期間記憶部
79
FLAG記憶部
99
比較手段
100
外部バスロック解除手段
101
不揮発性メモリ
96
外部バスロック手段
103
金額記憶部
98
カウントダウン・回数記憶部
102
外部バス制御部
比較手段
104
9A
送受信・整流・ロジック回路
4
カードリーダ／ライタ
3
ホストコンピュータ

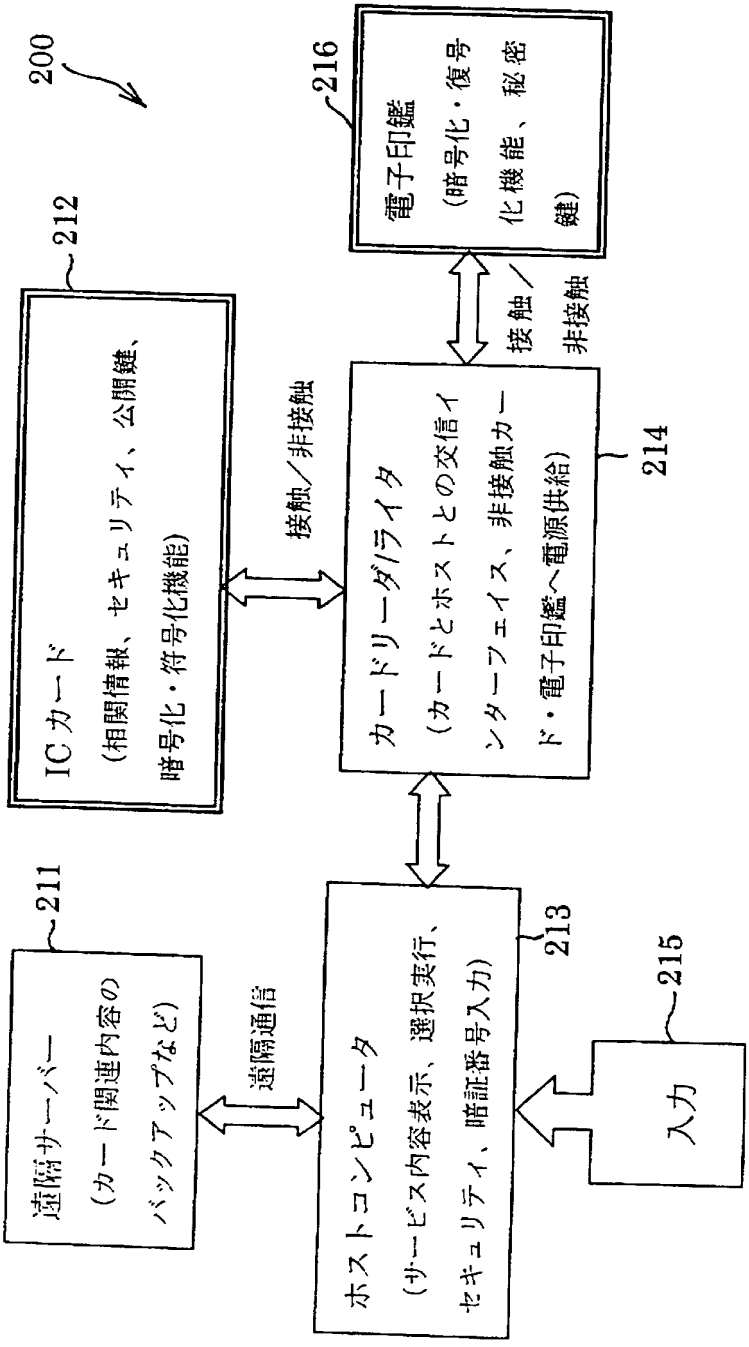
【図１２】


電子印鑑
携帯でカード課金
（暗証番号）
JR カード Suica
電話カード等
（カードのみ）
高級家電の盗難
防止（個人管理）
電子錠
（暗証番号）
携帯遠隔家電制御
（暗証番号）
車両防犯
（鍵）
カード現金引出し
（暗証番号）
書きとめ郵便配達
（伝統印鑑／サイン）
カード買い物
（目視署名）
パソコンアクセス
（暗証番号）
入退室管理
（カードのみ）
市役所
（伝統印鑑）
カードで給油・高速料
（カードのみ）

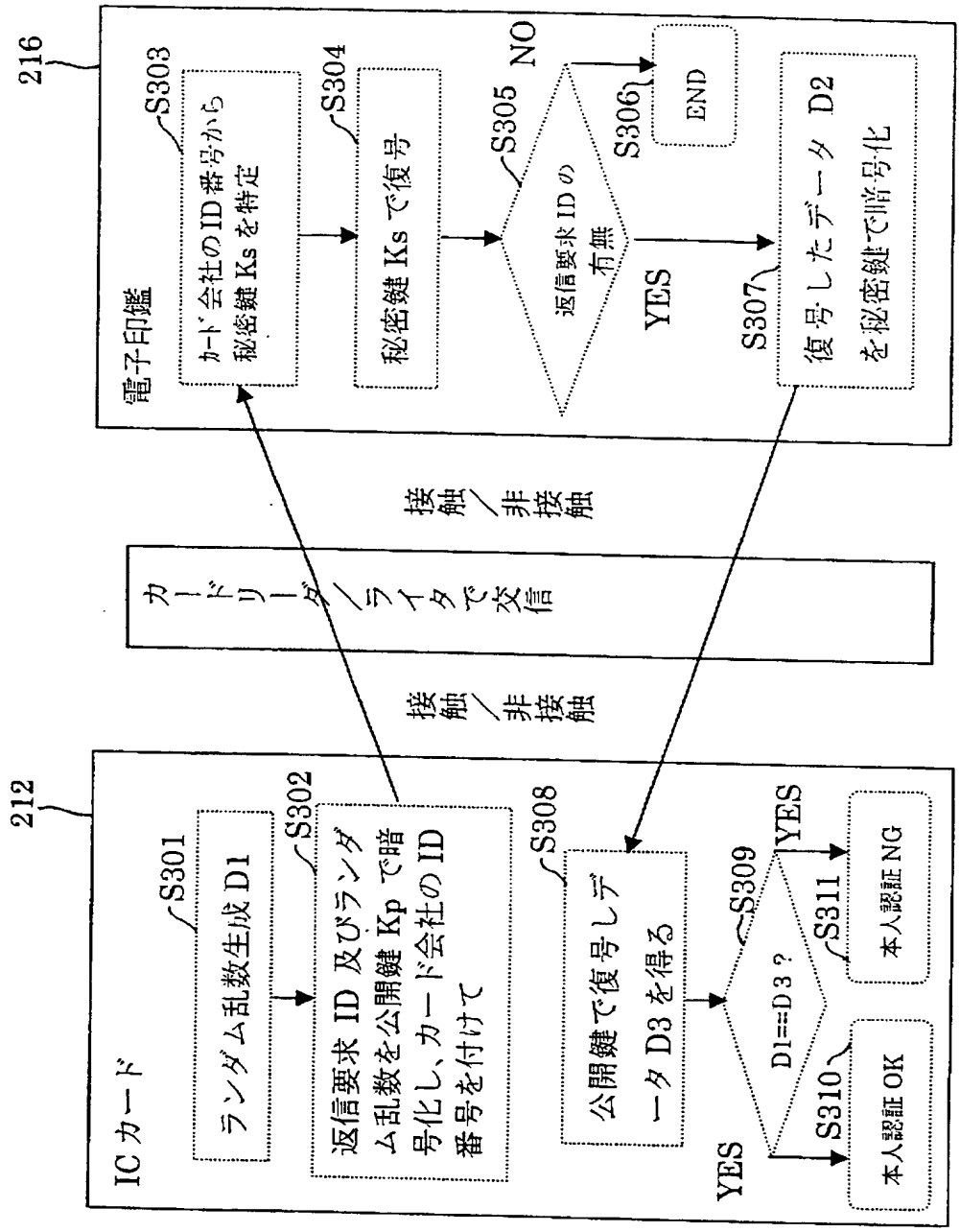
【図１３】


110
114
112
ICカード
接触／非接触
カードリーダ／
カードライタ
113
111
遠隔サーバ
遠隔通信
ホストコンピュータ
115
入力
装置

【図１４】


200
212
ICカード
(相関情報、セキュリティ、公開鍵、暗号化・符号化機能)
216
電子印鑑
(暗号化・復号化機能、秘密鍵)
接触／非接触
接触／非接触
カードリーダ/ライタ
(カードとホストとの交信インターフェイス、非接触カード・電子印鑑へ電源供給)
214
211
遠隔サーバー
(カード関連内容のバックアップなど)
遠隔通信
ホストコンピュータ
(サービス内容表示、選択実行、セキュリティ、暗証番号入力)
213
215
入力

【図１５】


216
電子印鑑
S303
カード会社のID番号から
秘密鍵Ksを特定
S304
秘密鍵 Ks で復号
S305
返信要求 ID の
有無
NO
S306
END
YES
S307
復号したデータ D2
を秘密鍵で暗号化
接触／非接触
カードリーダ／ライタで交信
接触／非接触
212
ICカード
S301
ランダム乱数生成 D1
S302
返信要求 ID 及びランダム乱数を公開鍵 Kp で暗号化し、カード会社の ID 番号を付けて
S308
公開鍵で復号しデータ D3 を得る
S309
D1==D3 ?
YES
S311
本人認証 NG
YES
S310
本人認証 OK

【書類名】　要約書

【要約】

【課題】電子印鑑にカード会社のＩＤ番号を組み込むことなく、電子印鑑を届印としてカードに登録することにより、ＩＣカードを容易に発行でき、かつ、従来の電子印鑑を用いないシステムに対して新たなる改造や増設をすることなく、電子印鑑とカードによる事前の本人認証により処理相手に電子印鑑を渡さずに、電子印鑑を高セキュリティでカードのアクセス保護に使用できる。

【解決手段】電子印鑑５または７側からカード６に対して交信要求（ＩＤ）を送信し、カード６はこれをチェックする。チェックがＯＫであれば、カード６の事前認証部のカードセキュリティ処理部６Ｂでは、ランダム乱数を発生させ、これを公開鍵で暗号化して、電子印鑑５側に送り、電子印鑑５はこの受け取ったデータを秘密鍵で復号化し、さらに秘密鍵で暗号化してカード６に送る。このデータを受け取ったカード６は、又公開鍵で復号化する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－２８９２２８
受付番号	５０２０１４７９１９０
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１４年１０月　２日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000005049
- 【住所又は居所】 大阪府大阪市阿倍野区長池町２２番２２号
- 【氏名又は名称】 シャープ株式会社

【代理人】 申請人
- 【識別番号】 100078282
- 【住所又は居所】 大阪市中央区城見１丁目２番２７号　クリスタルタワー１５階
- 【氏名又は名称】 山本　秀策

【選任した代理人】
- 【識別番号】 100062409
- 【住所又は居所】 大阪府大阪市中央区城見１丁目２番２７号　クリスタルタワー１５階　山本秀策特許事務所
- 【氏名又は名称】 安村　高明

【選任した代理人】
- 【識別番号】 100107489
- 【住所又は居所】 大阪市中央区城見一丁目２番２７号　クリスタルタワー１５階　山本秀策特許事務所
- 【氏名又は名称】 大塩　竹志

次頁無

特願２００２－２８９２２８

出　願　人　履　歴　情　報

識別番号　　［０００００５０４９］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　大阪府大阪市阿倍野区長池町２２番２２号
氏　名　　シャープ株式会社